



THÈMES VUIBERT UNIVERSITÉ
MATHÉMATIQUES

équations algébriques et théorie de galois

CLAUDE MUTAFIAN

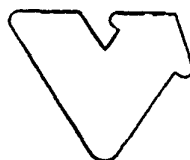
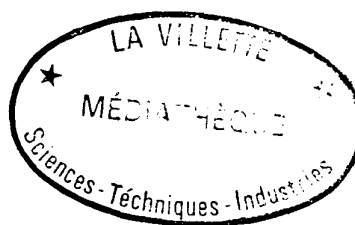




THÈMES VUIBERT UNIVERSITÉ
MATHÉMATIQUES

équations algébriques et théorie de galois

0 1 1
CLAUDE MUTAFIAN



Du même auteur

Algebra multilinear, productos tensoriales y exteriores, volume 16,5 × 22 cm, de 392 pages, cartonné; ouvrage en langue espagnole paru en février 1974 chez *Edicion revolucionaria, Instituto cubano del libro* (La Havane, Cuba).

A LA MÊME LIBRAIRIE

Le défi algébrique (premier et deuxième cycles universitaires).

- Tome 1 : *Semi-groupes, groupes*. — Vol. 16 × 24 cm, de 374 pages, relié.
- Tome 2 : *Anneaux, corps*. — Vol. 16 × 24 cm, de 348 pages, relié.

La structure vectorielle. — Vol. 15,5 × 24 cm, de 156 pages, broché.

Les applications linéaires. — Vol. 15,5 × 24 cm, de 276 pages, broché.

ISSN : 0224-7569
ISBN : 2-7117-2167-1

La loi du 11 mars 1957 n'autorisant, aux termes des alinéas 2 et 3 de l'article 41, d'une part que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale, ou partielle, faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause, est illicite » (alinéa 1^{er} de l'article 40).

Cette représentation ou reproduction par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles 425 et suivants du Code pénal.

© Librairie Vuibert, 1980.

Cette série de l'algèbre linéaire les uns des autres nécessaires à la différents sujets.

A partir du ni linéaire imaginal préparatoires au: comme de niveau aller plus loin da corps, les produi

Le style d'écrit en une suite de apparaître « natu des résultats pro extenso. Mais l'a reste à faire. Ceci

,5 x 22 cm, de
vriier 1974 chez
, Cuba).

4 pages, relié.
s, relié.
ché.
roché.

d'une part que les
n destinées à une
n but d'exemple et
le consentement de
(40).

stituerait donc une

rie Vuibert, 1980.

Introduction générale

Cette série de monographies présente des thèmes tous plus ou moins liés à l'algèbre linéaire. Il serait certes utopique de les considérer comme indépendants les uns des autres. Toutefois, en rappelant au besoin les résultats de base nécessaires à la compréhension de chacun, il s'avère possible de traiter les différents sujets comme des entités.

A partir du niveau du baccalauréat, la série couvre tous les sujets d'algèbre linéaire imaginables durant les deux premiers cycles universitaires et les classes préparatoires aux grandes écoles. Elle aborde aussi plusieurs thèmes considérés comme de niveau supérieur à la maîtrise, mais indispensables à quiconque veut aller plus loin dans des domaines proches de l'algèbre : ainsi les extensions de corps, les produits tensoriels, les classifications de transformations, etc.

Le style d'écriture a cherché à être le plus continu possible au lieu de consister en une suite de théorèmes et de corollaires. L'idée essentielle est de faire apparaître « naturellement » le pourquoi des notions introduites et le comment des résultats prouvés, le tout étant illustré de nombreux exemples traités *in extenso*. Mais l'ambition connaît ses limites : l'« algèbre pour tout le monde » reste à faire. Ceci est tout au plus une tentative d'« algèbre à visage humain »...

A Silvana MANGANO

Prologue

A un moment donné des études mathématiques, le professeur chuchotait d'un air mystérieux « on ne peut pas résoudre les équations à partir du degré cinq ». Cette affirmation, d'ailleurs vide de toute signification, se perdait ensuite dans un recoin de la mémoire : on n'avait pas l'occasion d'en savoir plus, vu que l'étude des équations algébriques ne figurait dans aucun programme jusqu'au troisième cycle. Les temps changent peu à peu, et il n'est plus rare d'entendre parler, en second cycle, d'extensions algébriques et de théorie de Galois.

Ceci dit, la littérature suit plus lentement, et il n'existe à ma connaissance aucun ouvrage de langue française consacré au sujet, en dehors bien sûr des classiques anciens. Cette théorie a tout au plus droit à un ou deux chapitres dans des cours d'algèbre généraux, comme application de l'étude des anneaux et des corps. Et encore, pas dans tous ! C'est pourtant l'une des branches les plus attachantes des mathématiques, non seulement à cause de la vie et de la mort « romantiques » du fondateur de la théorie, mais aussi pour des raisons en un sens esthétiques : tout se déroule de manière naturelle et « comme on peut l'espérer », en collant toujours à la réalité concrète, à savoir le calcul des racines d'une équation. Ainsi, la construction d'un polygone de 17 côtés résulte de la structure du groupe cyclique d'ordre 16, les deux études se font parallèlement.

Dans ces conditions, rien ne justifie l'« abstractification » qui domine dans la plupart des présentations. On part en général de la notion d'extension d'un corps K , puis on étudie les K -automorphismes de cette extension, et on applique le tout au cas du corps des racines d'un polynôme en constatant par miracle que ces racines sont permutées. Il est tout de même plus concret de partir du groupe des permutations des racines, pour constater que certaines peuvent se prolonger à tout le corps des racines, d'autres non ; les premières formeront le groupe de Galois, qui sera ainsi un sous-groupe du groupe des permutations des racines, et aussi — mais ce sera surtout là une constatation pratique — un sous-groupe du groupe des automorphismes du corps des racines.

Le fait que toute extension de degré fini soit simple, c'est-à-dire l'existence d'un élément primitif, est très utile même si l'on ne connaît pas explicitement un tel élément. Or le résultat est assuré si l'on est en caractéristique nulle, c'est-à-dire si les corps de base contiennent $\mathbb{Q}$. On fera l'hypothèse chaque fois qu'il le faudra, évitant ainsi les problèmes concernant la séparabilité. Il est plus important de savoir étudier une équation à coefficients entiers que de se demander ce qui se passe si les coefficients sont dans une extension transcendante d'un corps de caractéristique non nulle ! Dans ce dernier cadre apparaissent des problèmes techniques nouveaux qui masquent le déroulement de la théorie ; on les laisse pour des ouvrages plus spécialisés. Autrement dit, on pourra toujours ici diviser par des entiers non nuls, et les polynômes irréductibles n'auront pas de racines multiples. Sauf s'il est spécifié que l'on est dans tel cas particulier.

Cet ouvrage est donc exclusivement consacré à la théorie de Galois. Quel est l'arsenal supposé connu dès le départ ? Le moins possible : un peu sur les corps, un peu plus sur les groupes. Ce qui est nécessaire est rappelé au fur et à mesure, mais j'ai limité autant que possible les références à d'autres théories. Ainsi, on n'a pas besoin de connaître la théorie des anneaux et des idéaux.

Le mot « théorie de Galois » ne doit pas cacher le fait que les problèmes résolus sont tous pratiques. Et faire les calculs *in extenso* n'est pas se salir les mains. Bien que le calcul explicite d'un groupe de Galois et/ou des racines d'une équation soit en général hors de portée, il y a bien des cas — classiques ou plus ou moins « truqués » — où il peut être mené à bien sans trop de difficultés. Et alors un tel calcul est plus instructif que des pages de théories.

Note de l'Auteur

En 1949, dans *Riz amer*, une fille au corps splendide et au regard buté travaille dans les rizières de la plaine du Pô et rêve d'aventures en compagnie d'un « voyou ». Vingt-cinq ans plus tard, VISCONTI trouve en elle la parfaite incarnation d'une dame à l'air hautain et mystérieux surgissant dans la vie d'un compositeur mourant à Venise ou d'un vieux professeur confiné dans ses appartements. Silvana MANGANO, c'est à la fois ce symbole sexuel du néo-réalisme italien et l'image d'une aristocratie figée dans la beauté fascinante d'un passé révolu. Elle reste la « Grande Dame » du cinéma italien.

DES PROBLÈME

Bref rap,
Constru
Expressi
Racines
Les fonc
Transfor
Les équ
Les équ

LES EXTENSION

Degré d'
Éléments
Le polyn
Extensio
Quelques

GROUPE DE G

Bonnes e
Quelques
Les conj
Extensio
Groupe e

L'UTILISATION

Réduire
La corre
Des exer
Quelques
Le group
La carac
Construc

INDEX ALPHABÉ

INDEX DES NOT.

Galois. Quel est
 u sur les corps,
 ur et à mesure,
 es. Ainsi, on n'a

les problèmes
 pas se salir les
 es racines d'une
 ques ou plus ou
 icultés. Et alors

dans les rizières de la
 plus tard, Visconti
 argissant dans la vie
 partements. Silvana
 ne aristocratie figée
 cinéma italien.

Table des matières

DES PROBLÈMES HISTORIQUES	9
<i>Bref rappel</i>	10
<i>Constructions à la règle et au compas : le problème</i>	12
<i>Expression des racines d'une équation</i>	20
<i>Racines et corps de rupture</i>	27
<i>Les fonctions symétriques</i>	33
<i>Transformer une équation</i>	44
<i>Les équations de degré 3</i>	54
<i>Les équations de degré 4</i>	63
LES EXTENSIONS DE CORPS	69
<i>Degré d'une extension</i>	71
<i>Éléments algébriques sur un corps</i>	79
<i>Le polynôme minimum d'un élément algébrique</i>	90
<i>Extensions simples et éléments primitifs</i>	101
<i>Quelques corps de rupture</i>	117
GROUPE DE GALOIS D'UN POLYNÔME	129
<i>Bonnes et mauvaises permutations des racines</i>	134
<i>Quelques exemples de groupes de Galois</i>	144
<i>Les conjugués d'un élément algébrique</i>	162
<i>Extensions normales ou non</i>	184
<i>Groupe de Galois de l'équation générale</i>	193
L'UTILISATION DES GROUPES DE GALOIS	199
<i>Réduire le groupe de Galois</i>	200
<i>La correspondance de Galois</i>	212
<i>Des exemples</i>	217
<i>Quelques racines de l'unité</i>	227
<i>Le groupe de Galois d'une équation résoluble</i>	235
<i>La caractérisation des équations résolubles</i>	246
<i>Constructions à la règle et au compas : la solution</i>	254
INDEX ALPHABÉTIQUE	261
INDEX DES NOTATIONS	263

Des problèmes historiques

Le rôle des extensions de corps apparaît de manière assez naturelle dans l'étude de deux fameux problèmes historiques.

Le premier est celui de la construction à la règle et au compas : en ne disposant que d'une règle et d'un compas, et en partant de certains points du plan, quels sont ceux que l'on peut atteindre ?

Le second, plus difficile, est celui de la résolution des équations algébriques : les racines de

$$X^2 + pX + q$$

sont

$$\frac{-p \pm \sqrt{p^2 - 4q}}{2}$$

quand $p^2 - 4q$ a une racine carrée dans le corps de départ ; quelles sont les formules analogues donnant les racines d'équations de degré supérieur ?

Bref rappel

Dans cette étude, la plupart des corps utilisés seront les corps « usuels », c'est-à-dire $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ou plus généralement des sous-corps du corps $\mathbb{C}$ des complexes. Toutefois, on peut parfois pour le même prix se placer dans des cadres plus généraux, les exemples les plus classiques étant les corps d'entiers modulo un nombre premier donné : ce sont $\mathbb{Z}/2$, $\mathbb{Z}/3$, $\mathbb{Z}/5$,... La seule « différence » qui peut se produire avec les sous-corps de $\mathbb{C}$ est l'existence d'entiers n non nuls tels que l'élément $n1$ du corps soit nul.

Ainsi, 5 est nul dans $\mathbb{Z}/5$.

On reviendra plus loin brièvement sur ces anomalies.

A toute partie P d'un corps K correspond le sous-corps de K engendré par P , ou plus petit sous-corps de K contenant P .

- Le corps $\mathbb{Q}$ est engendré par n'importe quel rationnel non nul.
- Le corps $\mathbb{C}$ est engendré par $\mathbb{R}$ et $i = \sqrt{-1}$ ou, plus généralement, par $\mathbb{R}$ et tout complexe non réel.
- Le corps $\mathbb{Q}(X)$ des fractions rationnelles sur $\mathbb{Q}$, formé des quotients de polynômes, est engendré par $\mathbb{Q}$ et par l'indéterminée X ; il suffit même du seul X .
- Quel est le sous-corps de $\mathbb{C}$ engendré par i ? Il contient bien sûr 1, donc les sommes d'éléments égaux à 1, donc $\mathbb{N}$, mais alors aussi $\mathbb{Z}$ puis $\mathbb{Q}$. Il contient par suite les nombres complexes à parties réelle et imaginaire rationnelles et, comme ceux-ci forment un corps, c'est là le sous-corps engendré par i . On le note $\mathbb{Q}(i)$, il contient $\frac{3}{2} - \frac{i}{5}$ mais pas $\sqrt{2}$. On dit aussi que c'est le corps des nombres complexes à coordonnées rationnelles.

Si un corps contient K comme sous-corps, on dit que c'est une extension de K . Tout l'intérêt est que cette extension peut posséder des propriétés qui manquent à K .

- Dans $\mathbb{Q}$, 2 n'a pas de racine carrée. Il n'en a pas non plus dans les extensions $\mathbb{Q}(X)$ ou $\mathbb{Q}(i)$ ci-dessus décrites, mais il en a une dans l'extension $\mathbb{R}$.

- Toujours dans $\mathbb{Q}$, le polynôme $1 + X + X^2$ n'a pas de racine. Il n'en a ni dans $\mathbb{Q}(X)$, ni dans $\mathbb{R}$, ni dans $\mathbb{Q}(i)$, mais il en a deux dans $\mathbb{C}$, ce sont

$$j = \frac{-1 + i\sqrt{3}}{2} \quad \text{et son conjugué } \bar{j}.$$

Précisons donc que, bien souvent, on ne considérera que des corps extensions de $\mathbb{Q}$, ou corps contenant $\mathbb{Q}$: on inclut en particulier les sous-corps de $\mathbb{C}$ et les corps de fractions rationnelles à une ou plusieurs indéterminées sur ces corps.

Bref rappel

corps « usuels », c'est-à-dire $\mathbb{C}$ des complexes. dans des cadres plus d'entiers modulo un « différence » qui peut être n non nuls tels que

de K engendré par P ,

quel rationnel non nul.

$i = \sqrt{-1}$ ou, plus généralement, i réel.

es sur $\mathbb{Q}$, formé des coefficients et par l'indéterminée X ;

? Il contient bien sûr 1 , mais alors aussi $\mathbb{N}$, mais alors aussi les complexes à parties réelles. ceux-ci forment un corps. On le note $\mathbb{Q}(i)$, il

que c'est le corps des rationnels.

est une extension de K . propriétés qui manquent

il a pas non plus dans les entiers, mais il en a une

Constructions à la règle et au compas : le problème

On ne dispose que d'une règle, d'un compas et de certains points du plan. A partir de ceux-ci, quels sont les points que l'on peut « atteindre », c'est-à-dire obtenir comme intersection de deux cercles ou droites au bout d'un nombre fini (mais arbitraire) de constructions ?

La position du problème.

Soyons plus précis : le plan est identifié au corps $\mathbb{C}$ des complexes dont on se donne certains éléments, c'est-à-dire un sous-ensemble P .

A ce sous-ensemble on adjoint tous les points qui sont

- soit intersection de droites définies par les points de P ;
- soit intersection de cercles centrés en des points de P et de rayon égal à la distance de deux points de P ;
- soit intersection d'une droite de la première famille et d'un cercle de la seconde.

On obtient ainsi une partie P_1 contenant P .

Par exemple, si P est formé de deux points A et B , on obtient P_1 en adjoignant à P les symétriques de A par rapport à B et de B par rapport à A et les deux sommets des triangles équilatéraux de côté AB .

Si P est l'ensemble de trois points non alignés A , B et C , on construit P_1 en prenant les trois droites formant les côtés du triangle, et les neuf cercles centrés en l'un des points et de rayon égal à l'un des côtés du triangle. Les intersections de ces courbes donnent P_1 .

On passe alors au second stade ; à cette partie P_1 on fait subir le même sort, ce qui donne une partie P_2 plus grande. Et ainsi de suite... On obtient de cette manière une suite croissante $(P_n)_{n \in \mathbb{N}}$ de parties de $\mathbb{C}$, dont l'union $\bigcup_{n \in \mathbb{N}} P_n$ s'appelle l'ensemble des points **constructibles** à partir de P à l'aide de la règle et du compas.

Tout le problème est de trouver des conditions nécessaires ou suffisantes pour qu'un point soit constructible à partir de P .

Des exemples.

Le cas le plus simple consiste à partir d'un point et d'une unité de longueur, c'est-à-dire à prendre pour P l'ensemble $\{0, 1\}$.

L'ensemble des points constructibles à partir de 0 et 1 sera appelé ensemble des points constructibles (tout court) du plan, et sa détermination donne la réponse à ces fameux problèmes que sont

- la quadrature du cercle : chercher si π est un nombre constructible ;
- la duplication du cube ou construction d'un cube de volume double d'un cube donné : étudier la constructibilité du nombre $\sqrt[3]{2}$.

D'autres problèmes s'énoncent de manière analogue :

- la trisection de l'angle α n'est autre que la constructibilité de $\cos \frac{\alpha}{3}$ à partir de 0 et de $\cos \alpha$ (ou de $\sin \frac{\alpha}{3}$ à partir de 0 et de $\sin \alpha$, ce qui est équivalent car si on peut construire un cosinus on peut construire le sinus et réciproquement, pour des raisons évidentes).

Quelques constructions simples.

Commençons par étudier la structure algébrique des éléments constructibles à partir d'une partie P .

Rappelons que l'on peut tracer, à la règle et au compas :

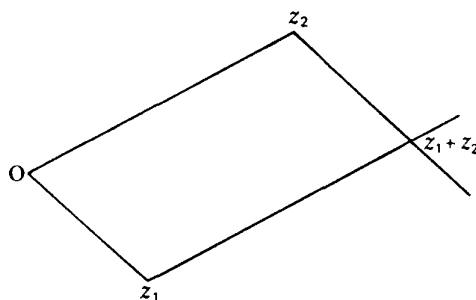
- la médiatrice de deux points ;
- la perpendiculaire à une droite, à partir d'un point donné ;
- la parallèle à une droite, à partir d'un point donné.

La construction effective est facile. On la laisse comme exercice.

On supposera toujours que la partie P contient 0 et 1, ce qui permet de construire à la règle et au compas l'axe réel et l'axe imaginaire.

Dans ces conditions, si z_1 et z_2 sont constructibles, on peut construire :

- la somme $z_1 + z_2$ de manière évidente ;

à la règle
problème

s points du plan.
dre », c'est-à-dire
d'un nombre fini

plexes dont on se

le rayon égal à la

d'un cercle de la

3. on obtient P_1 en
rt à B et de B par
s équilatéraux de

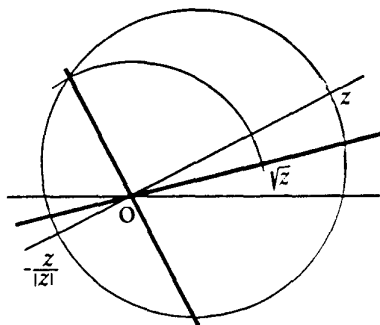
és A, B et C, on
nant les côtés du
oints et de rayon
ns de ces courbes

ir le même sort, ce
1 obtient de cette

on $\bigcup_{n \in \mathbb{N}} P_n$ s'appelle
ègle et du compas.
u suffisantes pour

sur l'axe réel à
de la droite
a alors même
x de z_1 et z_2 , et
t par l'origine.

et leur module commun, égal à $\sqrt{|z|}$, s'obtient à l'aide du cercle dont les extrémités du diamètre sont z et le point de module 1 sur la demi-droite opposée, c'est-à-dire $-\frac{z}{|z|}$.



Une première conclusion.

De tout ce qui précède, il résulte que, si l'on part d'une partie P contenant 1, l'ensemble des nombres constructibles à partir de P est

- un corps;
- stable par conjugaison;
- fermé par extraction de racines carrées, c'est-à-dire saturé par racines carrées.

C'est donc un corps contenant P et contenant les conjugués et les racines carrées de ses éléments.

Remarquons tout d'abord que, si l'on adjoint dès le départ à P ses conjugués, les nombres constructibles sont les mêmes et on peut alors se passer de la seconde condition.

On supposera donc désormais P symétrique par rapport à l'axe réel (ce qui, bien sûr, est le cas si P est formé de réels, en particulier si l'on part de 0 et 1 seulement).

Dans ces conditions, l'ensemble des sous-corps de $\mathbb{C}$ contenant P et saturés par racines carrées est non vide (car $\mathbb{C}$ convient) et l'intersection de tous possède les mêmes propriétés : il existe donc un plus petit sous-corps contenant P et saturé par racines carrées. Ce qui précède montre que le corps des nombres constructibles à partir de P contient ce corps. On va montrer qu'il lui est en fait égal.

Les intersections de droites et de cercles.

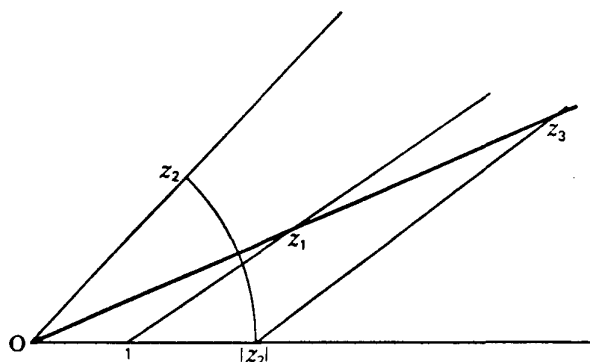
Pour cerner le problème, faisons les remarques suivantes :

L'équation de la droite passant par les points

$$z_1 = a + ib \quad \text{et} \quad z_2 = c + id$$

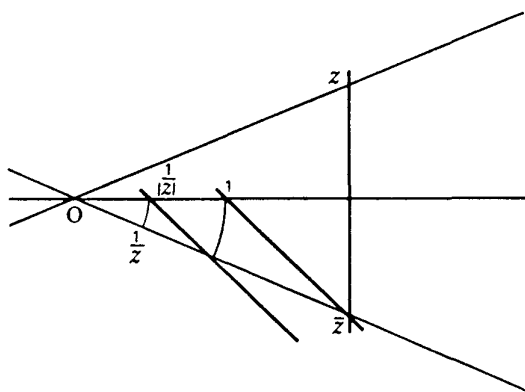
ont situées sur
e à construire)

• le produit $z_1 z_2$: son module se construit en « reportant » z_2 sur l'axe réel à l'aide d'un cercle, puis en traçant par le point obtenu, la parallèle à la droite joignant 1 et z_1 ; l'intersection z_3 avec la droite joignant O et z_1 a alors même module que $z_1 z_2$. Quant à l'argument de $z_1 z_2$, c'est la somme de ceux de z_1 et z_2 , et la construction est facile par un report d'arc sur un cercle passant par l'origine.



D'autre part, si z (supposé non nul) est constructible, on peut aussi construire :

- le conjugué $\bar{z}$, symétrique de z par rapport à l'axe réel ;
- la partie réelle et la partie imaginaire de z , intersections des deux axes avec leurs deux perpendiculaires menées par z ;
- l'opposé $-z$, en traçant la droite passant par O et z et en reportant de l'autre côté la longueur $|z|$ à l'aide du compas ;
- l'inverse $\frac{1}{z}$; pour cela on part de $\bar{z}$ et tout revient à construire sur la droite joignant O à $\bar{z}$ la longueur inverse de $|z|$, ce qui se fait facilement à l'aide de parallèles ;



- les deux racines carrées de z , opposées l'une de l'autre ; elles sont situées sur la bissectrice de l'axe réel et de la demi-droite joignant O et z (facile à construire)

CONSTRUCTIO

et leur module
extrémités du di

c'est-à-dire $-\frac{z}{|z|}$

Une première co

De tout ce qui
l'ensemble des n

- un corps ;
 - stable par co
 - fermé par e
- carrées.

C'est donc un
carrées de ses élé

Remarquons t
les nombres cons
condition.

On supposera
bien sûr, est le c
seulement).

Dans ces condi
racines carrées es
mêmes propriétés
par racines carr
constructibles à p
égal.

Les intersections

Pour cerner le

L'équation de !

est

$$(c - a)(y - b) - (d - b)(x - a) = 0.$$

Elle s'écrit donc sous la forme

$$ux + vy + w = 0$$

les réels u, v, w étant des sommes de produits de a, b, c, d , donc aussi de

$$z_1, \bar{z}_1, z_2, \bar{z}_2.$$

Passons à un cercle centré en $z = a + ib$ et de rayon R . Son équation est

$$(x - a)^2 + (y - b)^2 - R^2 = 0$$

et on l'écrit

$$x^2 + y^2 + ux + vy + w = 0$$

les réels u, v, w étant ici des sommes de produits de $z, \bar{z}, R$.

Dans ces conditions, partons d'une partie P symétrique par rapport à l'axe réel (donc stable par conjugaison). Cette partie engendre un sous-corps $K(P)$ de $\mathbb{C}$ qui contient le conjugué, la partie réelle et la partie imaginaire de tous ses éléments.

Deux droites définies par des points de P auront des équations de la forme

$$u_1x + v_1y + w_1 = 0 \quad \text{et} \quad u_2x + v_2y + w_2 = 0$$

tous les coefficients appartenant au corps $K(P)$ d'après ce qui précède. Leur intersection est donnée par la solution du système linéaire

$$\begin{cases} u_1x + v_1y + w_1 = 0 \\ u_2x + v_2y + w_2 = 0 \end{cases}$$

laquelle solution s'exprime à partir des coefficients à l'aide de sommes, produits, quotients, donc reste dans le corps $K(P)$.

Remplaçons maintenant la seconde droite par un cercle centré en un point de P et de rayon égal à la distance de deux points de P . Les intersections de la première droite et de ce cercle seront données par le système suivant :

$$\begin{cases} u_1x + v_1y + w_1 = 0 \\ x^2 + y^2 + u_3x + v_3y + w_3 = 0 \end{cases}$$

où tous les coefficients sont dans le corps $K(P)$. Pour le résoudre on peut « tirer » y de la première équation, le reporter dans la seconde, ce qui nous amène à

$$x^2 + sx + t = 0,$$

les réels s et t étant encore dans $K(P)$: il suffit de les exprimer à l'aide des coefficients du système. La résolution de cette équation fait intervenir les racines carrées de l'élément $\alpha = s^2 - 4t$, lequel α est encore dans $K(P)$. D'où la nécessité éventuelle d'« augmenter » $K(P)$ en considérant le sous-corps de $\mathbb{C}$ engendré non seulement par P , mais par P et une racine carrée de α . On obtient alors les valeurs de x , donc celles de y .

CON

En
inters
distailes co
rempi
précè

La ca

Fai
par ra
On
précè• 1
• 1
stricte
 $P_0 =$
saturé
• kMa
s'obti
d'un c
d'un c
saturé
Ces

(Li

Le sa

Po
rapp
satur
Or
croiss

Enfin, si l'on remplace la droite elle aussi par un cercle, on cherche les intersections de deux cercles, chacun centré en un point de P et de rayon égal à la distance de deux points de P . Le système s'écrit

$$\begin{cases} x^2 + y^2 + p_1x + q_1y + r_1 = 0 \\ x^2 + y^2 + p_2x + q_2y + r_2 = 0 \end{cases}$$

les coefficients étant toujours dans le corps $K(P)$ engendré par P . Il suffit de remplacer l'une des équations par la différence des deux pour se ramener au cas précédent.

La caractérisation algébrique de la constructibilité.

Faisons maintenant le point. On part d'une partie P contenant 1 et symétrique par rapport à l'axe réel, l'exemple le plus important étant le cas de $P_0 = \{0, 1\}$.

On considère alors les sous-corps suivants de $\mathbb{C}$, chacun contenant le précédent :

- le corps engendré par P , soit $K(P)$ (on aura ainsi $K(P_0) = \mathbb{Q}$);
- le plus petit corps contenant P et saturé par racines carrées; il est en général strictement plus grand que le précédent (comme le montre l'exemple de $P_0 = \{0, 1\}$ car le corps $\mathbb{Q}$ contient 2 mais pas ses racines carrées), on l'appelle le **saturé** de $K(P)$ par racines carrées;
- le corps des nombres constructibles à partir de P .

Mais on vient de voir que, si un nombre z est constructible à partir de P , il s'obtient à partir de $K(P)$ par un nombre fini d'opérations consistant à passer d'un corps à un corps plus grand engendré par le précédent et les racines carrées d'un de ses éléments. Il en résulte que z appartient à tous les corps contenant P et saturés par racines carrées, donc à leur intersection.

Ceci prouve l'égalité des deux derniers corps.

Les nombres constructibles à partir d'une partie du plan forment le plus petit corps contenant la partie et saturé par racines carrées.

(La partie est supposée symétrique par rapport à l'axe réel).

Le saturé par racines carrées.

Pour dire si $z \in \mathbb{C}$ est constructible à partir de P (supposé symétrique par rapport à l'axe réel), il faut donc savoir déterminer si z appartient ou non au saturé du corps $K(P)$ par racines carrées.

Or z appartiendra à ce saturé si, et seulement si, il existe une suite finie croissante de corps

$$K(P) \subset K_1 \subset K_2 \subset \dots \subset K_m$$

telle que

- z appartient à K_m ;
- pour tout i , le corps K_{i+1} est engendré par K_i et par un élément dont le carré est dans K_i .

En gros, on peut « atteindre » z en adjoignant successivement des racines carrées. On dit que K_{i+1} est extension de K_i par une racine carrée, et que K_m est extension de $K(P)$ par racines carrées successives. Le saturé d'un corps par racines carrées est donc l'union de ses extensions par racines carrées successives.

Une remarque : si K_{i+1} contient strictement K_i , il est engendré par K_i et les racines carrées d'un élément α de K_i qui n'est pas un carré dans K_i . Si l'on appelle $\sqrt{\alpha}$ l'une de ces racines carrées (l'autre étant $-\sqrt{\alpha}$), alors tout élément de K_{i+1} s'écrit de manière unique $a + b\sqrt{\alpha}$ avec a et b dans K_i , ce qui montre que K_{i+1} est de dimension 2 sur K_i , une base étant formée de 1 et $\sqrt{\alpha}$: on voit poindre l'algèbre linéaire... Tout ceci sera approfondi plus loin.

- Ainsi, partons du cas classique $P = \{0, 1\}$. Le corps engendré est $K(P) = \mathbb{Q}$, il n'est pas saturé par racines carrées.

- L'élément $\sqrt{2}$ n'est pas dans $\mathbb{Q}$, mais il est constructible, car le sous-corps de $\mathbb{C}$ engendré par $\mathbb{Q}$ et $\sqrt{2}$ est une extension par racine carrée.

- De même pour $\sqrt{2 + \sqrt{3}}$: on considère la chaîne $\mathbb{Q} \subset K_1 \subset K_2$ où K_1 est le sous-corps de $\mathbb{C}$ engendré par $\mathbb{Q}$ et $\sqrt{3}$, et K_2 le sous-corps engendré par K_1 et une racine carrée de $2 + \sqrt{3}$ (élément de K_1 sans racine carrée dans K_1) : ce corps K_2 est une extension de $\mathbb{Q}$ par racines carrées successives, donc il est contenu dans la saturation de $\mathbb{Q}$ par racines carrées.

- Pour $\sqrt[8]{2}$, on considérera la chaîne $\mathbb{Q} \subset K_1 \subset K_2 \subset K_3$ où K_1 est le sous-corps de $\mathbb{C}$ engendré par $\mathbb{Q}$ et $\sqrt{2}$, K_2 est engendré par K_1 et une racine carrée de $\sqrt{2} \in K_1$, K_3 engendré par K_2 et une racine carrée de $\sqrt[4]{2} \in K_2$. Le corps K_3 est extension de $\mathbb{Q}$ par racines carrées successives, et il contient $\sqrt[8]{2}$.

- Par contre, on verra plus tard que $\sqrt[3]{2}$ n'est pas constructible (à partir de 0 et 1), ce qui signifie qu'il n'appartient pas au saturé de $\mathbb{Q}$ par racines carrées, ou encore qu'il n'est dans aucune extension de $\mathbb{Q}$ par racines carrées successives : on ne peut pas l'« absorber » en adjoignant pas à pas des racines carrées.

- Les racines d'un polynôme pair de degré 4 sont constructibles : pour $X^4 + aX^2 + b$, on trouve les quatre racines

$$\pm \sqrt{\frac{-a \pm \sqrt{a^2 - 4b}}{2}},$$

qui s'expriment bien à l'aide de racines carrées seulement.

Une ren
éléments s
factorisabl
à dire qu'un
vérifie à l'a

Ou encc

Tout ce
problèmes

Exercices.

1. Con.

$$\sqrt{2}$$

2. Divis

3. Com

4. Cons
donc

5. A pa
Trad
Éten

6. L'ens
ratio

7. Véri
égale

En dé
donc

Une remarque : dire qu'un corps contient les racines carrées de tous ses éléments signifie que tout polynôme de degré 2 sur ce corps est totalement factorisable (c'est-à-dire produit de deux polynômes de degré 1), ce qui équivaut à dire qu'un tel polynôme possède une racine, ou encore qu'il est réductible. On le vérifie à l'aide du calcul classique :

$$X^2 + pX + q = \left(X + \frac{p}{2}\right)^2 - \frac{p^2 - 4q}{4}.$$

Un corps saturé par racines carrées est un corps sur lequel tout polynôme de degré 2 est réductible.

Ou encore :

La saturation d'un corps par racines carrées est la plus petite extension sur laquelle tout polynôme de degré 2 est réductible.

Tout ceci suppose que 2 est non nul dans le corps, ce qui ne pose pas de problèmes si l'on travaille dans le corps $\mathbb{C}$.

Exercices.

1. Construire à la règle et au compas le point $\sqrt{2 + \sqrt{3}}$ et le point $\sqrt{2 + \sqrt{3}} + i\sqrt[4]{2}$ à partir de 0 et 1.
2. Diviser à la règle et au compas un angle en deux angles égaux.
3. Comment peut-on diviser un segment en trois ?
4. Construire à la règle et au compas un carré de côté donné, un carré de surface donnée, un losange de côtés donnés.
5. A partir des réels a et b , construire les racines de $X^2 + aX + b$.
Traduction : construire deux nombres à partir de leur somme et de leur produit. Étendre au cas où a et b sont complexes.
6. L'ensemble des nombres complexes racines de polynômes non nuls à coefficients rationnels est saturé par racines carrées.
7. Vérifier que les deux nombres complexes suivants ont une puissance cinquième égale à 1 :

$$\frac{-1 + \sqrt{5}}{4} + i \frac{\sqrt{10 + 2\sqrt{5}}}{4} \quad \text{et} \quad \frac{-1 - \sqrt{5}}{4} + i \frac{\sqrt{10 - 2\sqrt{5}}}{4}.$$

En déduire que les racines du polynôme $X^5 - 1$ sont constructibles et que l'on peut donc construire à la règle et au compas un pentagone régulier.

ment dont le carré

ment des racines
rée, et que K_m est
d'un corps par
carrées successives.

ndré par K_i et les
 K_i . Si l'on appelle
élément de K_{i+1}
montre que K_{i+1}
on voit poindre

e corps engendré
carrées.

nstructible, car le
ne extension par

idère la chaîne
engendré par $\mathbb{Q}$ et
e racine carrée de
 K_1) : ce corps K_2
essives, donc il est
carrées.

$K_1 \subset K_2 \subset K_3$ où
et $\sqrt{2}$, K_2 est
 K_1 , K_3 engendré
Le corps K_3 est
et il contient $\sqrt[8]{2}$.

as constructible (à
it pas au saturé de
aucune extension
on ne peut pas
cines carrées.

nt constructibles :
ines

is seulement.

Expression des racines d'une équation

Un autre problème historique introduit naturellement l'étude des extensions de corps : c'est celui de la résolution des équations algébriques.

On montre, par diverses méthodes (dont — soit dit en passant — aucune n'est vraiment satisfaisante au point de vue démarche), que tout polynôme à coefficients complexes possède une racine dans le corps $\mathbb{C}$ des complexes, donc un nombre de racines égal à son degré (en comptant chaque racine avec son ordre de multiplicité).

Le problème est alors de calculer ces racines, c'est-à-dire de trouver une « formule » donnant ces racines en fonction des coefficients du polynôme.

Expressions rationnelles.

Que signifie la phrase précédente ? Prenons des nombres complexes, soit $a_1, \dots, a_n$ (qui seront les coefficients du polynôme, par exemple), ou même une famille infinie $(a_i)_{i \in I}$.

Une « formule » à partir des a_i sera une expression faisant intervenir les a_i et des « opérations » du corps $\mathbb{C}$. Lesquelles ?

Si l'on n'admet que les additions, soustractions, multiplications et quotients, les éléments que l'on « atteindra » à l'aide des a_i seront tous les éléments du corps engendré par les a_i : on dira que ces éléments s'expriment *rationnellement* en fonction des a_i .

Notons que tout sous-corps de $\mathbb{C}$ contient $\mathbb{Q}$ et que le corps engendré par les coefficients d'un polynôme sera $\mathbb{Q}$ lui-même si ces coefficients sont entiers (ou rationnels).

Équations binômes et radicaux.

Il est hors de question d'exprimer les racines d'un polynôme arbitraire à l'aide des coefficients si l'on ne s'autorise que ces opérations rationnelles. En d'autres termes, les racines d'un polynôme n'ont aucune raison d'appartenir au corps engendré par les coefficients.

Il suffit de considérer le polynôme $X^2 - 2$. Les racines $\pm \sqrt{2}$ sont hors du corps $\mathbb{Q}$ engendré par les coefficients 1 et -2 .

EXPRESSION

Les polynômes non nuls. En divisant par la racine 0) on élimine les racines n -ièmes de toutes les racines.

On notera son évidence d'ambiguïté où le choix de la racine habituelle concorde.

Une équation montre que si l'on a à partir des coefficients admettent les extrêmes au corps engendré par les coefficients.

Les radicaux binômes à coefficients

Les polynômes « les plus simples » sont ceux qui n'ont que deux coefficients non nuls. En divisant par une puissance adéquate de X (ce qui ne fait qu'éliminer la racine 0) on écrira ce polynôme sous la forme $X^n - d$. Les racines sont toutes les racines n -ièmes de d dans $\mathbb{C}$, elles s'obtiennent en multipliant l'une d'elles par toutes les racines n -ièmes de l'unité, soit $(1, e^{\frac{2i\pi}{n}}, e^{\frac{4i\pi}{n}}, \dots, e^{\frac{(n-1)i\pi}{n}})$.

On notera souvent $\sqrt[n]{d}$ l'une de ces racines n -ièmes de d , ce qui est une source évidente d'ambiguïtés : en fait, ou bien on utilisera ce symbole dans un contexte où le choix de la racine n'importe pas, ou bien on s'en remettra aux conventions habituelles concernant certains cas.

- En particulier, si d est un réel et si n est impair, il y a une seule racine n -ième réelle de d , c'est celle-là que l'on désigne en général par $\sqrt[n]{d}$.
- Autre cas : si d est un réel positif et si n est pair, il y a deux racines n -ièmes réelles de d opposées l'une de l'autre, et c'est à la racine positive que l'on associe le symbole $\sqrt[n]{d}$.
- Ainsi sont définis sans ambiguïté des symboles comme $\sqrt[3]{-5}$, $\sqrt[4]{2} - \sqrt[3]{3}$. Le symbole $\sqrt{-1}$ peut désigner i ou $-i$, on choisit en général i , ce qui donne par exemple pour $\sqrt{-3}$ le choix $i\sqrt{3}$.
- Par contre, une écriture comme $\sqrt[4]{-1}$ ne correspond à aucune convention de choix et désigne arbitrairement l'une des quatre racines quatrièmes de -1 : dangereux...

Une équation comme $X^n - d = 0$ s'appelle une **équation binôme**, et son étude montre que si l'on veut avoir une chance d'exprimer les racines de tout polynôme à partir des coefficients il faut au moins, outre les opérations rationnelles, admettre les extractions de racines n -ièmes, pour tout n , c'est-à-dire « adjoindre » au corps engendré par les coefficients les éléments qui ont une puissance dans ce corps.

Un élément ayant une puissance dans un corps donné s'appelle un radical relatif à ce corps.

Les radicaux relatifs à un corps sont donc toutes les racines des équations binômes à coefficients dans ce corps.

Les éléments d'un corps K sont bien sûr des radicaux relatifs à K , et ce sont les seuls dans le cas d'un corps comme $\mathbb{C}$ puisque ce dernier contient toutes les racines de ses polynômes.

Par contre, $\sqrt{2}$ ou i ou $1 + i$ sont des radicaux relatifs à $\mathbb{Q}$ sans être dans $\mathbb{Q}$: les deux premiers ont leur carré dans $\mathbb{Q}$, le troisième a pour carré $(1 + i)^2 = 2i$, donc pour puissance quatrième $(1 + i)^4 = -4 \in \mathbb{Q}$. L'élément $\sqrt{2} + i$, lui, n'est pas un radical relatif à $\mathbb{Q}$, car aucune de ses puissances n'est dans $\mathbb{Q}$; mais il s'exprime rationnellement à l'aide de radicaux relatifs à $\mathbb{Q}$.

Expressions algébriques.

Dans ces conditions, à partir de la famille d'éléments $(a_i)_{i \in I}$ du corps $\mathbb{C}$, il est logique de considérer non seulement les expressions rationnelles des a_i (c'est-à-dire les éléments du corps engendré), mais tous les complexes que l'on peut écrire à partir des a_i à l'aide d'opérations rationnelles et d'extractions de racines. On dira qu'un élément ainsi obtenu s'exprime *algébriquement* à l'aide des a_i .

Ainsi,

$$\sqrt{2} + i, \quad \sqrt[3]{1 + \sqrt{2}}, \quad \sqrt[3]{\frac{2 - \sqrt[4]{2}}{\sqrt{3}}} - \frac{1 + \sqrt[5]{3 + \sqrt{2}}}{\sqrt[4]{-5}}$$

s'expriment algébriquement à partir de $\mathbb{Q}$. On notera que chaque expression représente, comme on l'a vu, *plusieurs* nombres complexes.

Le nouveau problème sera alors le suivant : les racines d'un polynôme s'expriment-elles algébriquement à l'aide des coefficients ?

La réponse est bien sûr positive au degré 1 et aussi au degré 2, les racines de $X^2 + pX + q$ s'exprimant rationnellement à l'aide de p, q et des racines carrées de $p^2 - 4q$. On verra qu'elle est encore positive aux degrés 3 et 4, mais qu'à partir du degré 5 il y a des polynômes dont les racines ne s'expriment pas algébriquement à l'aide des coefficients.

La saturation d'un corps par radicaux.

L'adjonction à un corps K de tous ses radicaux, puis de toutes les expressions algébriques, donne une extension $\bar{K}$, que l'on peut voir, soit comme le corps des expressions algébriques sur K , soit comme le plus petit corps contenant K et contenant aussi tous les radicaux de ses éléments. On l'appelle **saturation par radicaux** de K .

Dans ces conditions, dire que les racines du polynôme P s'expriment algébriquement à l'aide des coefficients signifie que ces racines appartiennent à la saturation par radicaux du corps engendré par les coefficients : on dit aussi que l'équation $P = 0$ est **résoluble par radicaux**, ou encore résoluble tout court. En un sens, une équation résoluble par radicaux est une équation qui « se ramène » à la résolution d'un certain nombre d'équations binômes. Le corps engendré par ses racines doit alors être un sous-corps de la saturation par radicaux du corps engendré par ses coefficients.

Un commentaire.

Sil'on y regarde de plus près, pourquoi les radicaux ? En fait, l'idée générale est de ramener la résolution de l'équation $P = 0$ à celle d'un certain nombre

EXPRESSIO

d'équations
appellera d

Tout rev
d'équations
certains sy
rapport à c
racines de
résolvante
partielle sui

Tout dép
choisit les éc
aurait pu ch
symbole qu
équations se

Les extensio

Vu le rôle
besoin de c

L'idée se
K, s'exprim
chaîne finie

$a_i)_{i \in I}$ du corps $\mathbb{C}$, il est
nelles des a_i (c'est-à-
es que l'on peut écrire
ctions de racines. On
t à l'aide des a_i .

$$\frac{1 + \sqrt[5]{3 + \sqrt{2}}}{\sqrt[4]{-5}}$$

On notera que chaque
a, plusieurs nombres

cines d'un polynôme
?

et aussi au degré 2, les
nnellement à l'aide de
erra qu'elle est encore
r du degré 5 il y a des
pas algébriquement à

toutes les expressions
oit comme le corps des
corps contenant K et
appelle **saturation par**

onôme P s'expriment
ines appartiennent à la
ients : on dit aussi que
soluble tout court. En
ion qui « se ramène » à
Le corps engendré par
par radicaux du corps

fait, l'idée générale est
d'un certain nombre

d'équations d'un « type plus simple », soit $T_1 = 0, T_2 = 0, \dots, T_n = 0$, que l'on appellera des **résolvantes partielles** de $P = 0$.

Tout revient à préciser cette catégorie, c'est-à-dire à choisir une famille d'équations que l'on appellera « simples », et dont on notera les racines par certains symboles; dans ces conditions, une équation sera dite résoluble par rapport à cette famille si, et seulement si, ses racines s'expriment à l'aide des racines de ces équations « simples », donc de ces « symboles ». A chaque résolvante partielle, on « augmente » le corps, c'est-à-dire que la résolvante partielle suivante aura ses coefficients dans ce corps « augmenté ».

Ainsi, on montre que les racines de $X^4 + X^3 + X^2 + X + 1$ sont

$$\frac{-1 + \varepsilon_1 \sqrt{5}}{4} + \varepsilon_2 i \frac{\sqrt{10 + \varepsilon_1 2\sqrt{5}}}{4},$$

où ε_1 et ε_2 prennent les valeurs -1 ou $+1$. L'équation est donc résoluble à l'aide des résolvantes partielles « binômes » :

$$\begin{aligned} X^2 - 5 &= 0, \\ X^2 - (10 + 2\sqrt{5}) &= 0, \\ X^2 - (10 - 2\sqrt{5}) &= 0. \end{aligned}$$

Tout dépend du choix de la famille d'équations simples. Il se trouve que l'on choisit les équations binômes, et que l'on note $\sqrt[n]{\alpha}$ une racine de $X^n - \alpha$. Mais on aurait pu choisir, par exemple, la famille des équations $X^n + X + \alpha$, noter par un symbole quelconque, par exemple $\sqrt[n]{\alpha}$, une de ses racines et voir quelles équations se ramènent à des résolvantes partielles de cette forme...

Les extensions par radicaux.

Vu le rôle important joué par la saturation par radicaux d'un corps K , on a besoin de caractériser les éléments de cette saturation K_r .

Ainsi, l'élément $\alpha = \sqrt{2 - \sqrt[3]{3}}$ est dans la saturation par radicaux de $\mathbb{Q}$. Pour l'obtenir, on peut passer d'abord de $\mathbb{Q}$ au corps $\mathbb{Q}_1$ engendré par $\mathbb{Q}$ et $\sqrt[3]{3}$, puis de $\mathbb{Q}_1$ au corps $\mathbb{Q}_2$ engendré par $\mathbb{Q}_1$ et une racine carrée de $2 - \sqrt[3]{3} \in \mathbb{Q}_1$. On construit donc une chaîne $\mathbb{Q} \subset \mathbb{Q}_1 \subset \mathbb{Q}_2$ telle que chaque corps soit engendré par le précédent et un radical relatif à celui-ci, le dernier corps contenant notre élément α . Autrement dit, on adjoint « pas à pas » des radicaux.

L'idée se généralise immédiatement. Le fait que α , élément d'une extension de K , s'exprime algébriquement à partir de K signifie exactement qu'il existe une chaîne finie croissante de corps

$$K \subset K_1 \subset \dots \subset K_m$$

telle que :

- le corps K_m contient α ;
- pour tout i , le corps K_{i+1} est engendré par K_i et un radical t_i d'un élément de K_i ; on écrira alors

$$K_{i+1} = K_i(t_i).$$

On dit alors que K_{i+1} est **extension par radical** de K_i , et que K_m est extension de K par **radicaux successifs**.

La saturation par radicaux de K n'est autre que l'union de ses extensions par radicaux successifs : ce sont les éléments que l'on obtient en adjoignant « pas à pas » des radicaux.

L'analogie avec la construction à la règle et au compas est claire : la seule différence est qu'ici on s'autorise *tous* les radicaux, et pas seulement les racines carrées.

Le corps $\mathbb{C}$ est bien sûr extension de $\mathbb{R}$ par radical, mais on verra qu'il n'est pas extension de $\mathbb{Q}$ par radicaux successifs.

Les polynômes à coefficients rationnels.

La saturation par radicaux du corps $\mathbb{Q}$, ou de tout sous-corps de $\mathbb{C}$, est contenue dans $\mathbb{C}$, car $\mathbb{C}$ est lui-même saturé par radicaux. Mais l'inclusion peut être stricte.

Pour simplifier, bornons-nous aux polynômes à coefficients rationnels, le corps engendré par les coefficients étant alors $\mathbb{Q}$; tout ce qui suit se traduit d'ailleurs sans peine à des corps autres que $\mathbb{Q}$.

La clôture algébrique de $\mathbb{Q}$ est un sous-corps $\bar{\mathbb{Q}}$ de $\mathbb{C}$ contenant la saturation par radicaux $\mathbb{Q}_r$ de $\mathbb{Q}$: on a donc la situation $\mathbb{Q} \subset \mathbb{Q}_r \subset \bar{\mathbb{Q}} \subset \mathbb{C}$.

Notre problème est de savoir si les racines d'un polynôme à coefficients rationnels s'expriment algébriquement à l'aide de $\mathbb{Q}$, c'est-à-dire si ces racines sont dans $\mathbb{Q}_r$. Or, on verra plus tard que l'ensemble de *toutes* les racines des polynômes à coefficients rationnels forme un corps A , appelé corps des **nombre algébriques** sur $\mathbb{Q}$; ce corps A est bien sûr contenu dans $\bar{\mathbb{Q}}$, car $\bar{\mathbb{Q}}$ est algébriquement clos, et il contient $\mathbb{Q}_r$, car il est lui-même saturé par radicaux (si $\alpha \in A$ est racine de $P \in \mathbb{Q}[X]$, alors un radical comme $\sqrt[n]{\alpha}$ sera racine de $P(X^n) \in \mathbb{Q}[X]$, donc sera encore dans A). D'où la nouvelle situation

$$\mathbb{Q} \subset \mathbb{Q}_r \subset A \subset \bar{\mathbb{Q}} \subset \mathbb{C}.$$

La première inclusion est propre (considérer par exemple $\sqrt{2}$) ainsi que la dernière (on montre que π n'est pas dans la clôture algébrique de $\mathbb{Q}$). On verra plus loin, par contre, que A est en fait égal à $\bar{\mathbb{Q}}$ (voir p. 98).

Tout le problème de la résolution des équations est axé sur la seconde inclusion $\mathbb{Q}_r \subset A$: est-elle propre ou non ?

L'égalité $\mathbb{Q}_r = A$ signifierait exactement que toute racine d'un polynôme à coefficients rationnels s'exprime algébriquement à l'aide de $\mathbb{Q}$, ou encore que tout

nombre algébrique
à l'aide de
rationnels s'exprime
L'un des
malheureuse
qu'il existe

L'indépendance

En fait, dans
sont des lettres
« formules »
Mais qu'en
« rien à voir »
Si $X_1, \dots$
polynôme

De manière
on dira qu'il
indéterminé
si l'on note K
de $K(x_1, \dots)$
indéterminé
L'homom

est alors défini
($x_1, \dots, x_n$).
Bref, des
« peut consi

Par contre
polynôme
égalité s'appuie
aussi relati

On étend
algébrique

nombre algébrique s'exprime algébriquement (vocabulaire un peu malheureux...) à l'aide de rationnels. Dans ces conditions, toute équation à coefficients rationnels serait résoluble.

L'un des buts de ce texte est de montrer, non sans peine, qu'il n'en est malheureusement rien ! Ce corps $\mathbb{Q}$, est un sous-corps propre de A , c'est-à-dire qu'il existe des équations à coefficients rationnels non résolubles par radicaux.

On verra que c'est le cas par exemple du polynôme $X^5 - 4X - 2$, dont les racines ne s'expriment pas algébriquement à l'aide de $\mathbb{Q}$, alors que ce sont bien sûr des nombres algébriques.

L'indépendance algébrique.

En fait, dans l'étude théorique, on prendra des polynômes dont les coefficients sont des *lettres* : on recouvrira ainsi tous les cas, en substituant ensuite dans les « formules générales » les lettres par leurs valeurs.

Mais qu'entend-on par le mot « lettre » ? Ce sont des « éléments » qui n'ont « rien à voir » les uns avec les autres, le cas typique étant celui des indéterminées.

Si $X_1, \dots, X_n$ sont les indéterminées dans l'anneau $K[X_1, \dots, X_n]$, le seul polynôme nul en $(X_1, \dots, X_n)$ est le polynôme nul.

De manière analogue, si $x_1, \dots, x_n$ sont des éléments d'une extension L de K , on dira qu'ils sont **algébriquement indépendants** sur K si le seul polynôme à n indéterminées sur K nul en $(x_1, \dots, x_n)$ est le polynôme nul. En d'autres termes, si l'on note $K(x_1, \dots, x_n)$ le sous-corps de L engendré par K et les x_i , tout élément de $K(x_1, \dots, x_n)$ est la valeur en $(x_1, \dots, x_n)$ d'une *unique* fraction rationnelle à n indéterminées.

L'homomorphisme « évaluation en $(x_1, \dots, x_n)$ »

$$\begin{aligned} R &\rightarrow R(x_1, \dots, x_n) \\ K[X_1, \dots, X_n] &\rightarrow L \end{aligned}$$

est alors défini (car aucun dénominateur de fraction rationnelle ne s'annule en $(x_1, \dots, x_n)$, il est injectif, et son image est le corps $K(x_1, \dots, x_n)$).

Bref, des éléments algébriquement indépendants seront des éléments que l'on « peut considérer » comme autant d'indéterminées sur le corps.

Par contre, si $(x_1, \dots, x_n)$ sont algébriquement dépendants sur K , il existe un polynôme non nul $P \in K[X_1, \dots, X_n]$ vérifiant $P(x_1, \dots, x_n) = 0$: une telle égalité s'appelle une relation de **dépendance algébrique** sur K entre les x_i ; on dit aussi relation de **dépendance rationnelle**.

Ainsi, des relations de dépendance rationnelles entre $u = \sqrt{2}$ et $v = \sqrt{3}$ sur $\mathbb{Q}$ seront

$$u^2 - 2 = 0, \quad \text{ou} \quad v^2 - 3 = 0, \quad \text{ou} \quad u^2 + v^2 = 5.$$

On étend ces définitions sans difficultés à une famille infinie : la dépendance algébrique équivaut à la dépendance d'une sous-famille finie.

L'équation générale de degré n .

Dans ces conditions, on appellera **équation générale** de degré n sur $\mathbb{Q}$ l'équation $X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0 = 0$, où les a_i sont algébriquement indépendants sur $\mathbb{Q}$. Le problème de sa résolution consiste à exprimer ses racines à l'aide d'opérations rationnelles et de radicaux à partir du corps $\mathbb{Q}(a_0, a_1, \dots, a_{n-1})$ des fractions rationnelles à n indéterminées sur $\mathbb{Q}$, qui est le plus petit corps contenant les coefficients. On doit donc introduire la saturation par radicaux de ce corps, mais la difficulté provient de ce que le corps $\mathbb{Q}(a_0, a_1, \dots, a_{n-1})$ n'est plus sous-corps de $\mathbb{C}$. On ne peut donc pas partir de ce grand « fourre-tout » qu'est $\mathbb{C}$ pour ensuite le diminuer, il faut partir de ce que l'on a et l'augmenter.

C'est pourquoi, au lieu de faire la théorie sur les sous-corps de $\mathbb{C}$, on la fera (et ce n'est guère plus difficile) sur un corps K arbitraire (contenant $\mathbb{Q}$ en général).

Exercices.

1. Quels radicaux doit-on adjoindre à $\mathbb{Q}$ pour exprimer rationnellement les racines de

$$\frac{X^3 + 3X^2 + 3X + 2}{X^4 + X^2 + 1} \quad X^4 + 1 ?$$

2. Montrer que

$$1 + X + X^2 + X^3 + X^4$$

est irréductible sur $\mathbb{Q}$, et que ses racines sont les racines cinquièmes non réelles de l'unité. Peut-on les exprimer algébriquement sur $\mathbb{Q}$?

3. Vérifier que les expressions algébriques suivantes sont bien des nombres algébriques, c'est-à-dire que chacune est racine d'un polynôme sur $\mathbb{Q}$ à coefficients non nuls (l'ambiguïté des radicaux importe peu...) :

$$\sqrt{2} + \sqrt{3}, \quad \sqrt[3]{\frac{1 + \sqrt{2}}{3}}, \quad \sqrt[4]{\frac{3\sqrt[3]{2} - 1}{2}} + i\sqrt{3}.$$

4. Exprimer à l'aide de radicaux relatifs à $\mathbb{Q}$ les racines de l'unité d'ordre 2, 3, 4, 5, 6.
5. Un polynôme pair de degré 4 est toujours résoluble.

Par ra,
grand co
il existe
Plus p
racines d
démontre
algébriqu
près) : on

Le corps d

Si P est
corps eng
les racines
corps de d

On mon
de la clôt
importe... E
sera toujou
bien sûr de
On dira

degré n sur $\mathbb{Q}$
 ont algébrique-
 e à exprimer ses
 partir du corps
 sur $\mathbb{Q}$, qui est le
 ire la saturation
 e que le corps
 pas partir de ce
 partir de ce que

$\mathbb{C}$, on la fera (et
 t $\mathbb{Q}$ en général).

ment les racines de

èmes non réelles de

bien des nombres
 sur $\mathbb{Q}$ à coefficients

$\sqrt{3}$.

d'ordre 2, 3, 4, 5, 6.

Racines et corps de rupture

Par rapport à tous ses sous-corps, le corps $\mathbb{C}$ des complexes joue le rôle d'un grand corps dans lequel « tout se passe ». On montre en fait que pour tout corps il existe un « grand corps » jouant ce rôle.

Plus précisément, on appelle **algébriquement clos** tout corps contenant les racines de tous ses polynômes (voir le *Défi algébrique*, tome II, page 141). On démontre alors que pour tout corps K il existe un unique corps minimum algébriquement clos le contenant (l'unicité étant toujours aux isomorphismes près) : on l'appelle la **clôture algébrique** de K .

- Ainsi $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$, mais pas celle de $\mathbb{Q}$: il y a des sous-corps propres de $\mathbb{C}$ qui sont algébriquement clos, et le plus petit d'entre eux est la clôture algébrique de $\mathbb{Q}$.
- Aucun corps de fractions rationnelles n'est algébriquement clos, car le corps $K(X)$ ne contient pas de racine carrée de X .
- De même, aucun corps fini n'est algébriquement clos car, pour un tel corps F , le polynôme $1 + \prod_{\alpha \in F} (X - \alpha)$ vaut 1 en tout point de F , donc n'a pas de racine dans F .

Le corps de rupture d'un polynôme.

Si P est un polynôme sur K , on prend dans la clôture algébrique de K le sous-corps engendré par K et les racines de P . C'est le corps minimum contenant K et les racines de P , on l'appelle **corps de rupture** de P sur K (on dit parfois plutôt **corps de décomposition** ou **corps des racines**).

On montre en fait que l'on peut définir ce corps de rupture indépendamment de la clôture algébrique (voir le *Défi algébrique*, tome II, page 297). Mais peu importe... En tout cas, quand on parlera désormais des racines de $P \in K[X]$, il sera *toujours* sous-entendu que l'on se place dans le corps de rupture de P (ou bien sûr dans une extension de ce dernier...).

On dira aussi que c'est le corps de rupture de l'équation $P = 0$.

- Le corps de rupture de $1 + X^2$ sur $\mathbb{R}$ est $\mathbb{C}$ tout entier, alors que son corps de rupture sur $\mathbb{Q}$ est $\mathbb{Q}(i)$, corps des nombres complexes à parties réelle et imaginaire rationnelles.

• Le corps de rupture de $X^2 + aX + b$ sur $\mathbb{Q}$ est engendré par une racine carrée de $a^2 - 4b$. C'est $\mathbb{Q}$ si $a^2 - 4b$ est un carré dans $\mathbb{Q}$, alors que, dans le cas contraire, c'est un $\mathbb{Q}$ -espace de dimension 2, une base étant donnée par 1 et une racine carrée de $a^2 - 4b$ dans $\mathbb{C}$.

• Les racines cubiques de l'unité autres que 1 dans $\mathbb{C}$ sont

$$j = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \quad \text{et} \quad \bar{j} = j^2$$

donc le corps de rupture de $X^3 - 1$ sur $\mathbb{Q}$ est engendré par j , ou encore par $i\sqrt{3}$ (fait que l'on retrouve en remarquant que c'est aussi le corps de rupture de $\frac{X^3 - 1}{X - 1} = X^2 + X + 1$). Il est formé des nombres complexes $a + ib\sqrt{3}$, avec a et b rationnels.

• Le corps de rupture d'une équation binôme $X^n - \alpha = 0$ est engendré par K , une racine n -ième de α , et toutes les racines n -ièmes de l'unité. C'est donc aussi le corps engendré par une racine n -ième de α et le corps de rupture de $X^n - 1 \in K[X]$.

• Pour l'équation binôme $X^n - 1$, le corps de rupture sur $\mathbb{Q}$ est appelé **corps cyclotomique** d'indice n . Il est engendré par les n racines n -ièmes de l'unité, dont les $(n - 1)$ autres que 1 sont les racines de

$$1 + X + X^2 + \dots + X^{n-1}.$$

On montre que les racines sont les $e^{\frac{2ik\pi}{n}}$, avec $k = 0, 1, \dots, n - 1$, ce sont donc les puissances de $\omega = e^{\frac{2i\pi}{n}}$, sommets d'un polygone régulier de n côtés. Aussi

$$X^n - 1 = 0$$

s'appelle-t-elle une équation de la division du cercle.

Factorisation d'un polynôme.

Résultat classique : si $P \in K[X] \setminus 0$ possède une racine α dans une extension L de K , il existe $Q \in L[X]$ vérifiant

$$P = (X - \alpha)Q.$$

En recommençant, au cas où Q admet aussi α pour racine, on arrive à l'existence de $T \in L[X]$ vérifiant

$$P = (X - \alpha)^m T \quad \text{et} \quad T(\alpha) \neq 0.$$

On dit que m est l'**ordre de multiplicité** de la racine α ; la racine est dite simple pour $m = 1$, multiple pour $m \geq 2$.

Si n est le degré de P , celui de T est $n - m$, donc la somme des ordres de

RACINE

multiplic.
si, l'exten
est totale
totale

Quand
une fois c
égal à soi
toute am

Corps de

On a n
fonction
extension
La con

• le co
radicaux
• il exi
coefficient

Quelques

1° On
considère
2° Si l'
diminuer

En part
quitte à d
3° Plus
l'étude de
degrés str

est engendré par
est un carré dans
un $\mathbb{Q}$ -espace de
racine carrée de

dans $\mathbb{C}$ sont

engendré par j , ou
arquant que c'est
 $+ X + 1$). Il est
 a et b rationnels.

e $X^n - \alpha = 0$ est
toutes les racines
engendré par une
 $X^n - 1 \in K[X]$.

rupture sur $\mathbb{Q}$ est
engendré par les n
tres que 1 sont les

les $e^{\frac{2ik}{n}}$, avec
nces de $\omega = e^{\frac{2i\pi}{n}}$,
Aussi

1 cercle.

ns une extension L

acine, on arrive à

cine est dite simple

me des ordres de

multiplicité des racines de P ne peut dépasser n . Elle sera égale à n si, et seulement si, l'extension L contient le corps de rupture de P sur K , auquel cas on dit que P est **totalelement factorisable** dans L . Dans $L[X]$, on écrit alors la factorisation totale

$$P = a(X - \alpha_1)^{m_1} \dots (X - \alpha_r)^{m_r}.$$

Quand on dit « soit $\beta_1, \dots, \beta_s$ les racines du polynôme R », on écrit parfois une fois chaque racine, mais parfois aussi on répète chacune un nombre de fois égal à son ordre de multiplicité. Dans ce dernier cas on parle, si l'on veut éviter toute ambiguïté, de la *famille* des racines de R .

Ainsi, le polynôme $(X^2 + 1)^2(X - 2)^3 \in \mathbb{Q}[X]$ a pour racines
 $i, -i, 2$, mais la famille de ses racines s'écrit

$$(i, i, -i, -i, 2, 2, 2).$$

Corps de rupture d'une équation résoluble.

On a montré que les racines du polynôme P s'expriment algébriquement en fonction des coefficients si, et seulement si, elles sont contenues dans une extension par radicaux successifs du corps engendré par les coefficients.

La condition s'énonce encore de l'une des manières suivantes :

- le corps de rupture du polynôme P est contenu dans la saturation par radicaux du corps engendré par les coefficients de P ;
- il existe une extension par radicaux successifs du corps engendré par les coefficients, dans laquelle le polynôme est totalement factorisable.

Quelques remarques sur les racines d'un polynôme et la réductibilité.

1° On peut toujours, en divisant par le coefficient dominant, se borner à considérer des polynômes dont le coefficient dominant vaut 1.

2° Si l'on connaît une racine α d'un polynôme P , on peut en profiter pour diminuer le degré en divisant par $X - \alpha$ ou une de ses puissances.

Ainsi, l'équation binôme $X^n - 1 = 0$ possède 1 pour racine, son étude se ramène à celle des racines du polynôme

$$\frac{X^n - 1}{X - 1} = 1 + X + \dots + X^{n-1}.$$

En particulier, on peut toujours supposer le terme constant de P non nul, quitte à diviser par une puissance de X (ce qui ne fait qu'éliminer la racine 0).

3° Plus généralement, si P est réductible sur le corps K , on écrit $P = QR$, et l'étude de l'équation $P = 0$ se ramène à l'étude des équations $Q = 0$ et $R = 0$, de degrés strictement inférieurs.

4° On ne change pas le corps de rupture en divisant (si c'est possible) ou en multipliant par des polynômes ayant toutes leurs racines dans le corps de départ : tout revient à enlever ou à adjoindre des racines qui sont dans ce corps de départ.

De même, on peut supprimer les exposants d'une factorisation si l'on cherche le corps de rupture : celui de $P^n Q^m$ est le même que celui de PQ .

- Si l'on part de

$$P = 1 + X^2 + X^4 \in \mathbb{Q}[X]$$

multiplions par $T = X^2 - 1$. On ne change pas le corps de rupture et on remplace P par

$$TP = (X^2 - 1)(X^4 + X^2 + 1) = X^6 - 1.$$

Le corps de rupture de P est donc engendré par les racines sixièmes de l'unité, donc par

$$e^{\frac{2i\pi}{6}} = e^{\frac{i\pi}{3}} = \frac{1 + i\sqrt{3}}{2};$$

c'est encore le corps engendré par $i\sqrt{3}$, formé des complexes $a + ib\sqrt{3}$ avec a et b rationnels.

- Le polynôme

$$P = 1 + X + X^2 + X^3 \in \mathbb{Q}[X]$$

s'annule pour -1 , son corps de rupture est celui de

$$R = \frac{P}{X+1} = X^2 + 1, \text{ c'est le corps } \mathbb{Q}(i) \text{ des complexes à coordonnées rationnelles.}$$

5° Il arrive souvent que l'on ait à considérer, dans $\mathbb{Q}[X]$, un polynôme à coefficients entiers, soit $P \in \mathbb{Z}[X]$.

On démontre (c'est dû au caractère d'anneau « factoriel » de $\mathbb{Z}$) que, pour que P soit irréductible dans $\mathbb{Q}[X]$, il suffit qu'il le soit dans $\mathbb{Z}[X]$, c'est-à-dire qu'il n'existe pas de polynôme R et S non constants à coefficients entiers vérifiant $P = RS$.

Vient un autre critère suffisant, celui dit d'Eisenstein : si P est encore à coefficients entiers, si le coefficient dominant vaut 1 et si les autres ont un facteur premier commun p dont le carré ne divise pas $P(0)$, alors P est irréductible dans $\mathbb{Z}[X]$, donc dans $\mathbb{Q}[X]$ (voir *Le Défi algébrique*, tome II, page 214).

Ainsi $X^6 - 3X^2 + 6X + 15$ est irréductible dans $\mathbb{Q}[X]$.

L'existence de racines multiples.

Un résultat classique permet, sans connaître les racines d'un polynôme $P \in K[X]$, d'affirmer s'il possède ou non des racines multiples (dans son corps de rupture bien sûr).

RACINES

En effet, et de P' , pol donc les rac seulement :

P n'a

C'est là u carré de po séparable.

On devr que des rac car on peut T' : il a les r

En effet, les racines multiples de P sont exactement les racines communes de P et de P' , polynôme dérivé de P (voir *Le Défi algébrique*, tome II, page 133), ce sont donc les racines du P.G.C.D. de P et P' . Or ce P.G.C.D. n'aura pas de racine si, et seulement si, il est constant. D'où l'équivalence :

P n'a que des racines simples $\Leftrightarrow P$ et P' sont premiers entre eux.

C'est là un important critère pratique. Il signifie que P n'est divisible par aucun carré de polynôme dans son corps de rupture. On dit alors parfois que P est **séparable**.

- Le dérivé de

$$X^3 + pX + q \in \mathbb{Q}[X]$$

est $3X^2 + p$. Le P.G.C.D. des deux est aussi celui de $X^2 + \frac{p}{3}$ et du

reste de la division euclidienne de $X^3 + pX + q$ par $X^2 + \frac{p}{3}$, lequel reste est

$$X^3 + pX + q - X\left(X^2 + \frac{p}{3}\right) = \frac{2p}{3}X + q.$$

Or $3X^2 + p$ et $2pX + 3q$ sont premiers entre eux si, et seulement si, soit p est nul et q non nul, soit p est non nul et $-\frac{3q}{2p}$ non racine de $3X^2 + p$. La seconde condition s'écrit

$$3(9q^2) + p(4p^2) \neq 0$$

c'est-à-dire

$$4p^3 + 27q^2 \neq 0$$

ce qui inclut d'ailleurs la première condition. C'est donc là la condition de séparabilité du polynôme $X^3 + pX + q$.

- Si l'on reprend l'équation binôme $X^n - 1 = 0$ sur un corps K arbitraire, le dérivé de $X^n - 1$ est nX^{n-1} . Si n est non nul dans le corps K (ce qui est le cas si K contient le corps $\mathbb{Q}$), alors 0 est seule racine de nX^{n-1} et n'est pas de racine de $X^n - 1$.

Le polynôme $X^n - 1$ n'aura alors que des racines simples, et il y aura bien n racines n -ièmes de l'unité dans K .

- De même, si K contient $\mathbb{Q}$, il y aura n racines n -ièmes à tout élément non nul x de K , ce qui signifie que le symbole $\sqrt[n]{x}$ représente exactement n éléments (dans le corps de rupture de $X^n - x$ sur K ou dans toute extension) : il faut parfois choisir...

On devra parfois supposer que les polynômes avec lesquels on travaille n'ont que des racines simples. En caractéristique nulle, cela ne pose pas de problème, car on peut remplacer le polynôme T par le quotient de T et du P.G.C.D. de T et T' : il a les mêmes racines que T et toutes sont simples. Mais, si le corps de base ne

contient pas $\mathbb{Q}$, ce n'est pas toujours possible et, encore une fois, on ne s'en embarrassera pas.

Ainsi, en caractéristique 2, soit α sans racine carrée dans le corps K . Le polynôme $X^2 - \alpha$ a une racine double $\sqrt{\alpha}$ dans le corps de rupture, car tout élément est égal à son opposé, mais aucun polynôme sur K n'a $\sqrt{\alpha}$ comme racine simple, puisque $\sqrt{\alpha}$ n'est pas dans K . Ceci est dû au fait que le dérivé de $X^2 - \alpha$ est nul.

Un cas particulier est donné par un polynôme P irréductible sur K . Son dérivé P' , s'il n'est pas nul, est de degré strictement inférieur à celui de P , de même que tous ses diviseurs, donc aucun de ceux-ci ne peut diviser P : il en résulte que P et P' sont premiers entre eux, et P n'a que des racines simples. Reste le cas où P' est nul. Si le corps K contient $\mathbb{Q}$, la nullité de P' exige que P soit constant, et, comme il est non nul, il n'a pas de racine multiple.

On a montré, quand le corps K contient $\mathbb{Q}$:

Un polynôme irréductible n'a que des racines simples.

Attention au cas où K ne contient pas $\mathbb{Q}$: il y a beaucoup de peaux de banane, mais on ne s'en occupera pas ici.

Le polynôme $X^2 \in \mathbb{Z}/2[X]$ a un dérivé nul sans pour cela être constant.

Exercices.

1. Montrer que le corps de rupture de

$$X^4 - 2 \in \mathbb{Q}[X]$$

contient i , donc qu'il contient le corps $\mathbb{Q}(i)$ des complexes à coordonnées rationnelles, c'est donc un espace vectoriel sur $\mathbb{Q}(i)$, on vérifiera que la dimension est 4.

2. L'équation générale de degré n n'a que des racines simples.
3. Quel est le corps de rupture de

$$X^4 + aX^2 + b \in \mathbb{Q}[X] ?$$

Celui de $X^4 - 1 \in \mathbb{Q}[X]$, de $X^5 - 1 \in \mathbb{Q}[X]$, de $X^6 - 1 \in \mathbb{Q}[X]$?
Dans chaque cas, trouver la dimension comme $\mathbb{Q}$ -espace.

4. Montrer que, pour tout $n \in \mathbb{N}$, le polynôme

$$X^n + X + 1 \in \mathbb{Q}[X]$$

n'a que des racines simples.

Étudier de même

$$X^n + X + \alpha \quad \text{et} \quad X^n + X^2 + 1.$$

Le pro
donné, p
et pas d
Un éc
famille d
d'un poi

Les rela

Partoi

les coeffi
des coeff
On su
répète d
Le co
rupture,

En dé
« relatio

Une f
d'apparte
formées :

S HISTORIQUES

fois, on ne s'en

e carrée dans le
ouble $\sqrt{\alpha}$ dans le
son opposé, mais
e simple, puisque
dérivé de $X^2 - \alpha$

sur K. Son dérivé
e P, de même que
en résulte que P et
ste le cas où P' est
instant, et, comme

simples.

peaux de banane,

ns pour cela être

xes à coordonnées
ra que la dimension

[?] ?

Les fonctions symétriques

Le problème de départ, à savoir trouver des éléments annulant un polynôme donné, peut paraître un peu « parachuté » : pourquoi considérer des polynômes et pas d'autres types de fonctions ?

Un éclairage plus « naturel » apparaît quand on considère les propriétés de la famille des racines, c'est-à-dire non pas quand on cherche, une à une, les racines d'un polynôme, mais quand on étudie les diverses relations qui les lient.

Les relations entre coefficients et racines.

Partons d'un polynôme

$$P = a_0 + a_1X + \cdots + a_nX^n$$

les coefficients a_i étant dans un corps K (dont le plus petit candidat est le corps des coefficients, engendré par les a_i).

On suppose a_n non nul, et on appelle $(x_1, \dots, x_n)$ la *famille* des racines (on répète donc les racines suivant leur ordre de multiplicité).

Le corps de rupture est alors engendré par K et les x_i et, dans ce corps de rupture, on écrit l'égalité

$$a_0 + a_1X + \cdots + a_nX^n = a_n(X - x_1)(X - x_2) \cdots (X - x_n).$$

En développant le second membre, on trouve les n égalités suivantes, dites « relations entre coefficients et racines » :

$$x_1 + x_2 + \cdots + x_n = -\frac{a_{n-1}}{a_n}$$

$$\sum_{i < j} x_i x_j = \frac{a_{n-2}}{a_n}$$

$$\sum_{i < j < k} x_i x_j x_k = -\frac{a_{n-3}}{a_n}$$

.....

$$x_1 x_2 \cdots x_n = (-1)^n \frac{a_0}{a_n}.$$

Une première conséquence : bien que les racines n'aient aucune raison d'appartenir au corps des coefficients, les expressions du premier membre, formées à partir des racines, appartiennent à ce corps des coefficients.

Polynômes symétriques élémentaires.

Étant donné n indéterminées sur un corps K , on appelle **polynômes symétriques élémentaires** les n polynômes suivants :

- somme des indéterminées, soit $\sum_{i=1}^n X_i$;
- somme des produits deux à deux des indéterminées, soit $\sum_{i < j} X_i X_j$;
-
- somme des produits p à q des indéterminées, soit

$$\sum_{1 \leq i_1 < i_2 < \dots < i_p \leq n} X_{i_1} X_{i_2} \dots X_{i_p};$$

- produit des indéterminées, qui n'est autre que la somme des produits n à n (car il y a un seul tel produit).

On appellera $\sigma_1, \sigma_2, \dots, \sigma_n$ ces n polynômes.

Fonctions symétriques élémentaires.

Les valeurs de ces n polynômes sur une famille de n éléments s'appellent les **fonctions symétriques élémentaires** de ces éléments.

On a montré :

Les fonctions symétriques élémentaires des racines d'un polynôme appartiennent au corps engendré par les coefficients.

Une conséquence :

- la résolution d'une équation algébrique se ramène à celle d'un système (bien sûr non linéaire...) de n équations à n inconnues.

- Ainsi, les racines x_1 et x_2 de $X^2 + aX + b$ sont caractérisées par

$$\begin{cases} x_1 + x_2 = -a \\ x_1 x_2 = b. \end{cases}$$

- Au degré 3, appelons (x_1, x_2, x_3) la famille des racines de $X^3 + pX + q$. Elle est caractérisée par les trois égalités

$$\begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1 x_2 + x_1 x_3 + x_2 x_3 = p \\ x_1 x_2 x_3 = -q. \end{cases}$$

Si l'on connaît une racine u , les deux autres ont pour somme $-u$

Résoudre une équation

Dès lors, on peut résoudre une équation algébrique en connaissant les racines.

Plus précisément, on peut être justifié : si $x_1, \dots, x_n$ sont des racines d'un polynôme, alors $\alpha_1, \dots, \alpha_n$ en sont aussi.

Il est alors naturel de se demander si le corps engendré par les racines est plus grand que celui engendré par les coefficients. Le polynôme

$$X^n - \alpha_1^n$$

En d'autres termes, si l'on connaît n éléments d'un corps, peut-on trouver des fonctions symétriques élémentaires de ces éléments ? Et une équation algébrique sera une extension de ce corps.

Fractions rationnelles

En généralisant, on appelle **fraction** une expression de la forme

et pour produit $-\frac{q}{u}$ (ceci suppose u non nul, ce qui est assuré si q est non nul). Elles sont donc racines de

$$X^2 + uX - \frac{q}{u}$$

d'où la factorisation

$$X^3 + pX + q = \frac{1}{u}(X - u)(uX^2 + u^2X - q).$$

On reviendra plus loin sur l'étude de l'équation du troisième degré.

Résoudre une équation : l'autre interprétation.

Dès lors, on peut présenter autrement le problème de la résolution d'une équation algébrique : dans un certain « grand corps » on cherche n inconnues connaissant les valeurs de leurs n fonctions symétriques élémentaires.

Plus précisément, étant donné des éléments $\alpha_1, \dots, \alpha_n$ dans un corps K (qui peut être justement le corps engendré par les α_i), on cherche des éléments $x_1, \dots, x_n$ dont les fonctions symétriques élémentaires soient respectivement $\alpha_1, \dots, \alpha_n$. En général, il n'existera pas dans le corps K de tels éléments.

Ainsi, il n'existe pas de couple d'éléments de $\mathbb{Q}$ dont les fonctions symétriques élémentaires (somme et produit, en l'occurrence) soient 0 et 1.

Énoncé équivalent : $X^2 + 1$ ne se factorise pas sur $\mathbb{Q}$.

Il est alors naturel d'essayer d'augmenter le corps K , en cherchant dans un corps plus grand, L , des éléments dont les fonctions symétriques élémentaires soient les α_i . Le plus petit corps L qui convient sera bien sûr le corps de rupture du polynôme

$$X^n - \alpha_1 X^{n-1} + \alpha_2 X^{n-2} + \dots + (-1)^{n-1} \alpha_{n-1} X + (-1)^n \alpha_n.$$

En d'autres termes, la résolution d'une équation algébrique est la recherche de n éléments d'une extension d'un corps K , connaissant leurs n fonctions symétriques élémentaires, qui sont dans ce corps K .

Et une équation sera résoluble quand la saturation par radicaux du corps K sera une extension « assez grande », c'est-à-dire fournira les n solutions.

Fractions rationnelles symétriques.

En généralisant le cas des polynômes symétriques élémentaires, il est naturel d'appeler **fraction rationnelle symétrique** à n indéterminées toute fraction

rationnelle $R \in K(X_1, \dots, X_n)$ vérifiant

$$R(X_{p(1)}, \dots, X_{p(n)}) = R(X_1, \dots, X_n)$$

pour toute permutation p de n éléments.

Bien entendu, les n polynômes élémentaires $\sigma_1, \dots, \sigma_n$ en sont un cas particulier, ainsi que toute fraction rationnelle obtenue en substituant $\sigma_1, \dots, \sigma_n$ aux indéterminées : quelle que soit

$$T \in K(X_1, \dots, X_n)$$

la fraction rationnelle $T(\sigma_1, \dots, \sigma_n)$ est symétrique. On va maintenant montrer que, réciproquement, toute fraction rationnelle symétrique s'exprime rationnellement à l'aide des polynômes symétriques élémentaires.

En particulier, il en résultera :

Toute fonction rationnelle symétrique des racines d'un polynôme est dans le corps de base.

Plus précisément, soit $P \in K[X]$ un polynôme, $(x_1, \dots, x_n)$ la famille de ses racines, et S une fraction rationnelle symétrique à n indéterminées : alors $S(x_1, \dots, x_n)$ est dans K (bien que, répétons-le, les x_i n'aient aucune raison d'être dans K). Ceci suppose bien entendu que le dénominateur de S ne s'annule pas sur la famille des racines.

Ainsi, soit (x_1, x_2, x_3) les racines de $X^3 + pX + q$. La fonction symétrique $\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3}$ s'écrit

$$\frac{x_1x_2 + x_2x_3 + x_1x_3}{x_1x_2x_3}.$$

Elle vaut donc $-\frac{p}{q}$ (q est supposé non nul pour que 0 ne soit pas racine).

L'expression des polynômes symétriques.

Les polynômes symétriques élémentaires sont exactement les polynômes symétriques homogènes dont le degré partiel par rapport à chaque indéterminée vaut 1.

Ceci dit, on veut montrer que, si $\sigma_1, \dots, \sigma_n$ sont ces polynômes symétriques élémentaires, toute fraction rationnelle symétrique s'écrit $T(\sigma_1, \dots, \sigma_n)$ pour une certaine fraction rationnelle T . Ce qui signifie que $\sigma_1, \dots, \sigma_n$ engendrent le corps des fractions rationnelles symétriques.

Il suffit de le montrer pour les polynômes symétriques et même, simplement, pour les polynômes symétriques homogènes.

Un tel polynôme s'obtient en partant d'un monôme $X_1^{a_1} \dots X_n^{a_n}$ et en lui ajoutant les monômes différents obtenus en remplaçant la suite des indices des indéterminées par toutes les autres suites.

On l'écrira s

Ainsi, les élé

σ

D'autres « s »
qu'une indéter

somme des pu
On vérifie a

• En un pre
 σ_i . Il y a plusi
pratique, cons

P

Les racines

Dérivons pa
On trouve

d'où

La division

$\bar{Y}$

On multipli

$$\frac{Y'P'(Y)}{P(Y)}$$

Posons enfir

$$\frac{P'\left(\frac{1}{X}\right)}{XP\left(\frac{1}{X}\right)} =$$

On l'écrira symboliquement

$$\Sigma X_1^{z_1} \dots X_m^{z_m}.$$

Ainsi, les élémentaires sont

$$\sigma_1 = \Sigma X_i, \quad \sigma_2 = \Sigma X_i X_j, \quad \dots, \quad \sigma_n = X_1 \dots X_n.$$

D'autres « simples » sont ceux obtenus en partant d'un monôme ne comptant qu'une indéterminée. On posera

$$S_i = \Sigma X_i^i$$

somme des puissances i -ièmes des indéterminées.

On vérifie aisément

$$S_1 = \sigma_1 \quad S_2 = \sigma_1^2 - 2\sigma_2.$$

• En un premier stade, on va montrer que tous les S_i sont des polynômes en les σ_i . Il y a plusieurs méthodes. L'une d'entre elles, peut-être artificielle mais très pratique, consiste à partir du polynôme

$$P(Y) = Y^n - \sigma_1 Y^{n-1} + \sigma_2 Y^{n-2} + \dots + (-1)^n \sigma_n.$$

Les racines de ce polynôme en Y sont justement les X_i , ce qui s'écrit

$$P(Y) = (Y - X_1) \dots (Y - X_n).$$

Dérivons par rapport à Y .

On trouve

$$P'(Y) = \frac{P(Y)}{Y - X_1} + \dots + \frac{P(Y)}{Y - X_n}$$

d'où

$$\frac{P'(Y)}{P(Y)} = \frac{1}{Y - X_1} + \dots + \frac{1}{Y - X_n}.$$

La division suivant les puissances croissantes donne, pour tout entier q

$$\frac{1}{Y - X_i} = \frac{1}{Y} + \frac{X_i}{Y^2} + \dots + \frac{X_i^{q-1}}{Y^q} + \frac{X_i^q}{Y^q} \frac{1}{Y - X_i}.$$

On multiplie par Y et on fait la somme pour tous les $\frac{1}{Y - X_i}$. Il reste

$$\frac{YP'(Y)}{P(Y)} = n + \frac{S_1}{Y} + \frac{S_2}{Y^2} + \dots + \frac{S_{q-1}}{Y^{q-1}} + \frac{1}{Y^{q-1}} \left[\sum_i \frac{X_i^q}{Y - X_i} \right].$$

Posons enfin $X = \frac{1}{Y}$, pour arriver à

$$\frac{P\left(\frac{1}{X}\right)}{XP\left(\frac{1}{X}\right)} = n + S_1 X + S_2 X^2 + \dots + S_{q-1} X^{q-1} + X^q \left[\sum_i \frac{X_i^q}{1 - XX_i} \right].$$

On obtient donc les S_i en effectuant la division suivant les puissances croissantes de deux polynômes dont les coefficients sont fonction des σ_j . Plus précisément, on peut calculer

$$\frac{YP'(Y)}{P(Y)} = \frac{nY^n - (n-1)\sigma_1 Y^{n-1} + (n-2)\sigma_2 Y^{n-2} + \cdots + (-1)^{n-1} \sigma_{n-1} Y}{Y^n - \sigma_1 Y^{n-1} + \sigma_2 Y^{n-2} + \cdots + (-1)^n \sigma_n}.$$

La transformation $X = \frac{1}{Y}$ conduit au quotient

$$\frac{n - (n-1)\sigma_1 X + (n-2)\sigma_2 X^2 + \cdots + (-1)^{n-1} \sigma_{n-1} X^{n-1}}{1 - \sigma_1 X + \sigma_2 X^2 + \cdots + (-1)^n \sigma_n X^n}$$

et la somme $S_i = \sum X_j^i$ est le coefficient de X^i dans la division suivant les puissances croissantes (ou développement en série entière) du numérateur par le dénominateur.

Ainsi, les premiers termes de la division sont

$$n + \sigma_1 X + (\sigma_1^2 - 2\sigma_2)X^2 + (\sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3)X^3 + \cdots$$

d'où l'on tire

$$S_1 = \sigma_1 \text{ (heureusement)}$$

$$S_2 = \sigma_1^2 - 2\sigma_2$$

$$S_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3.$$

Le résultat s'utilise aussi dans des cas concrets. Par exemple, la somme des puissances quatrièmes des racines de $X^3 - 2X^2 + 1$ est le coefficient de X^4 dans le développement en série de

$$\frac{3 - 4X}{1 - 2X + X^3} = 3 + 2X + 4X^2 + 5X^3 + 8X^4 + \cdots.$$

On trouve la valeur 8.

• Une fois montré que, pour tout entier i , la somme des puissances i -ièmes des indéterminées est un polynôme en les polynômes symétriques élémentaires, on passe à un polynôme symétrique homogène arbitraire.

Il suffit de remarquer les égalités

$$S_p S_q = S_{p+q} + \sum X_1^p X_2^q \quad \text{pour} \quad p \neq q$$

$$(S_p)^2 = S_{2p} + 2 \sum X_1^p X_2^p$$

qui montrent que les polynômes $\sum X_1^p X_2^q$ sont des polynômes en les S_i , donc en les σ_j .

En les multipliant par S_i , on voit de même que

$$\sum X_1^p X_2^q X_3^r$$

a la même propriété. Et ainsi de suite...

On a bic

On dém
l'indépenda

Exemple.

En prati
démonstrat
symétriques
donnée. Ap

ant les puissances
nction des σ_i . Plus

$$\frac{+ (-1)^{n-1} \sigma_{n-1} Y}{- 1)^n \sigma_n}$$

$$\frac{1}{\sigma_{n-1} X^{n-1}}$$

division suivant les
du numérateur par le

nt

$$\sigma_2 + 3\sigma_3)X^3 + \dots$$

)

σ_3 .

crets. Par exemple, la
es de $X^3 - 2X^2 + 1$
nent en série de

$$X^3 + 8X^4 + \dots$$

puissances i -ièmes des
ques élémentaires, on

$\neq q$

ômes en les S_i , donc

On a bien montré :

Tout polynôme symétrique est un polynôme en les polynômes symétriques élémentaires.

On démontre en plus l'unicité d'une telle représentation, qui traduit l'indépendance algébrique de $\sigma_1, \dots, \sigma_n$ sur K (à vérifier).

Exemple.

En pratique, on ne passera pas forcément par les S_i en suivant la démonstration ci-dessus, on cherchera souvent à former, à partir des polynômes symétriques élémentaires, des expressions se rapprochant le plus de l'expression donnée. Après quoi on rectifie le tir...

Prenons, pour $n = 3$, la fraction rationnelle symétrique

$T = \sum \frac{X_1}{X_2}$. Elle comporte six termes, et s'écrit explicitement

$$T = \frac{X_1}{X_2} + \frac{X_2}{X_1} + \frac{X_1}{X_3} + \frac{X_3}{X_1} + \frac{X_2}{X_3} + \frac{X_3}{X_2}$$

Le dénominateur commun est $\sigma_3 = X_1 X_2 X_3$ et on calcule

$$T = \frac{\sum X_1^2 X_2}{\sigma_3}$$

On va comparer le numérateur au polynôme

$$\sigma_1 \sigma_2 = (\sum X_1)(\sum X_1 X_2) = \sum X_1^2 X_2 + 3X_1 X_2 X_3$$

d'où il résulte l'égalité

$$\sum X_1^2 X_2 = \sigma_1 \sigma_2 - 3\sigma_3$$

et l'expression finale

$$\sum \frac{X_1}{X_2} = \frac{\sigma_1 \sigma_2}{\sigma_3} - 3.$$

Une conséquence : si x_1, x_2, x_3 sont les racines de l'équation

$$X^3 - 3X^2 - X + 5,$$

on peut, sans les calculer, écrire l'égalité

$$\frac{x_1}{x_2} + \frac{x_2}{x_1} + \frac{x_1}{x_3} + \frac{x_3}{x_1} + \frac{x_2}{x_3} + \frac{x_3}{x_2} = \frac{3 \times (-1)}{-5} - 3 = \frac{-12}{5}.$$

Une application : le résultant de deux polynômes.

Soit P et Q des polynômes sur K ; appelons $(\alpha_1, \dots, \alpha_n)$ et $(\beta_1, \dots, \beta_m)$ les familles respectives de racines (dans le corps de rupture de PQ par exemple). La condition nécessaire et suffisante pour que P et Q aient une racine commune s'écrit

$$\prod_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} (\alpha_i - \beta_j) = 0.$$

Appelons $R(P, Q)$ l'expression $\prod (\alpha_i - \beta_j)$. Cette expression est symétrique par rapport aux α_i d'une part, aux β_j d'autre part, c'est donc un élément du corps engendré par les coefficients de P et Q .

On l'appelle le **résultant** des deux polynômes P et Q . Il s'écrit aussi, en utilisant les décompositions

$$P(X) = u \prod_{i=1}^n (X - \alpha_i) \quad \text{et} \quad Q(X) = v \prod_{j=1}^m (X - \beta_j)$$

sous l'une des formes :

$$R(P, Q) = \frac{1}{v^n} \prod_{i=1}^n Q(\alpha_i) = \frac{(-1)^{nm}}{u^m} \prod_{j=1}^m P(\beta_j).$$

On retiendra qu'au signe près, et pour des polynômes à coefficient dominant égal à 1, le résultant est le produit des valeurs d'un des polynômes sur la famille des racines de l'autre. En fait, on prendra souvent le résultant comme défini à un facteur non nul près.

On dit aussi que $R(P, Q) = 0$ est l'expression obtenue en éliminant l'indéterminée X entre P et Q .

Une remarque utile : on peut ajouter à l'un des polynômes un multiple scalaire de l'autre sans changer le résultat (toujours à des multiples non nuls près).

Mieux : si P et Q ont une racine commune, il en est de même de Q et R où R est le reste de la division euclidienne de P par Q , et réciproquement ; or le couple (Q, R) est plus facile que le couple (P, Q) , pour raisons de degrés.

- Pour éliminer X entre

$$X^2 + aX + b \quad \text{et} \quad X^2 + \alpha X + \beta$$

on écrit leur différence

$$(a - \alpha)X + b - \beta.$$

Si l'on suppose $a \neq \alpha$, le résultant s'obtient en prenant la valeur de l'un des polynômes en $-\frac{b - \beta}{a - \alpha}$. On trouve

$$R = [(b - \beta)^2 + (a - \alpha)(a\beta - b\alpha)]$$

(à un facteur non nul près toujours).

Un cas par la nullité cor résultant jou reviendra (v

Le déterminant

Un moyen « déterminant

La remarque et B (dans un K) équivaut appelant U

avec les rela:

Et il est facile de tels polynômes entre eux (car de degré).

Dès lors, si U et V l'équi

A et B ont u

C'est encore valable dans le cas $a = \alpha$: l'existence d'une racine commune équivaut à $b = \beta$, donc à $R = 0$.

• Le résultant de $X^n - 1$ et de $X^m - 1$ est nul puisque 1 est une racine commune.

Exclure 1 revient à considérer

$$\Omega_n = 1 + X + \dots + X^{n-1} \quad \text{et} \quad \Omega_m = 1 + X + \dots + X^{m-1}.$$

Une racine commune sera un $z \neq 1$ vérifiant

$$z^n = 1 \quad \text{et} \quad z^m = 1.$$

Mais les racines n -ièmes et m -ièmes de l'unité sont exactement les racines d -ièmes, où d est le P.G.C.D. de n et m :

$$\left. \begin{matrix} z^n = 1 \\ z^m = 1 \end{matrix} \right\} \Leftrightarrow z^d = 1.$$

La condition est donc : $d \neq 1$.

Conclusion : le résultant de Ω_n et Ω_m est nul si n et m ne sont pas premiers entre eux, égal à un sinon (toujours à des facteurs non nuls près).

Un cas particulier : le résultant d'un polynôme et de son dérivé, résultant dont la nullité correspond à l'existence d'une racine multiple du polynôme donné. Ce résultant joue un rôle spécial, on l'appelle le **discriminant** du polynôme ; on y reviendra (voir p. 205).

Le déterminant de Sylvester.

Un moyen « systématique » de calculer le résultant utilise la méthode dite « déterminant de Sylvester ».

La remarque de départ est la suivante : l'existence d'une racine commune à A et B (dans une extension contenant les deux corps de rupture sur le corps de base K) équivaut au fait que le P.G.C.D. de A et B est de degré supérieur à 1 ; en appelant U et V les quotients de A et B par ce P.G.C.D., on trouve l'égalité

$$VA - UB = 0$$

avec les relations

$$d^0 U < d^0 A \quad \text{et} \quad d^0 V < d^0 B.$$

Et il est facile de voir, à l'aide du théorème de Gauss, que réciproquement l'existence de tels polynômes U et V dans $K[X]$ entraîne que A et B ne sont pas premiers entre eux (car s'ils l'étaient, A diviserait U, ce qui est incompatible avec les raisons de degré).

Dès lors, si n et p sont les degrés de A et B, on trouve en écrivant les polynômes U et V l'équivalence suivante :

A et B ont une racine commune $\Leftrightarrow$
les polynômes A, XA, ..., $X^{p-1}A$, B, XB, ..., $X^{n-1}B$
sont linéairement dépendants sur K.

Écrivons

$$A = a_0 + a_1X + \dots + a_nX^n \quad \text{et} \quad B = b_0 + b_1X + \dots + b_pX^p.$$

La condition est la dépendance linéaire des $(n+p)$ vecteurs lignes suivants de K^{n+p} :

$$\begin{pmatrix} a_0 & a_1 & \dots & a_n & 0 & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_{n-1} & a_n & 0 & \dots & 0 \\ 0 & 0 & a_0 & a_1 & \dots & a_{n-2} & a_{n-1} & a_n & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ b_0 & b_1 & \dots & b_p & 0 & 0 & \dots & 0 \\ 0 & b_0 & \dots & b_{p-1} & b_p & 0 & 0 & \dots & 0 \\ 0 & 0 & b_0 & \dots & b_{p-2} & b_{p-1} & b_p & 0 & \dots & 0 \end{pmatrix}$$

Les p premières lignes et les n dernières sont chacune décalées d'un rang par rapport à la précédente.

L'existence d'une racine commune à A et B équivaut donc à la nullité du déterminant d'ordre $n+p$ de cette matrice.

Le déterminant s'appelle **déterminant de Sylvester** des deux polynômes, et il est, bien sûr, égal au résultant (toujours au signe et aux coefficients dominants près).

Il va sans dire qu'avant de le calculer on aura intérêt à abaisser les degrés, en remplaçant le couple (A, B) à l'aide de combinaisons linéaires ou de divisions euclidiennes : ainsi le résultant de A et B est le même que celui de B et B_1 , où B_1 est le reste de la division euclidienne de A par B (pourquoi ?).

Pour

$$X^2 + aX + b \quad \text{et} \quad X^2 + \alpha X + \beta,$$

le déterminant « brut » de Sylvester est d'ordre 4 et égal à

$$\begin{vmatrix} b & a & 1 & 0 \\ 0 & b & a & 1 \\ \beta & \alpha & 1 & 0 \\ 0 & \beta & \alpha & 1 \end{vmatrix}.$$

On peut remplacer le couple de polynômes par l'un d'eux et leur différence $(a-\alpha)X + b-\beta$, d'où le déterminant d'ordre 3 :

$$\begin{vmatrix} b & a & 1 \\ b-\beta & a-\alpha & 0 \\ 0 & b-\beta & a-\alpha \end{vmatrix} = (b-\beta)^2 + (\alpha-\alpha)(a\beta - b\alpha)$$

que l'on déduit d'ailleurs facilement du précédent.

Retour sur la résolution des équations.

D'après ce qui précède, non seulement les fonctions symétriques *élémentaires* des racines d'un polynôme $P \in K[X]$ sont dans le corps des coefficients, mais aussi *toutes* les fonctions rationnelles symétriques de ces racines.

Le prob
« récupérer
leurs fonct

Exercices.

1. Expr
fracti

2. Expr

à l'ai
En d
racir

puis

3. Écri
que
deux

4. Calc

ains.

5. En a

En

$S_p =$

$S_p =$

(les

6. Si n
fona

Le problème de la résolution d'une équation algébrique est donc celui de « récupérer », dans une extension adéquate, des inconnues à partir du corps de leurs fonctions rationnelles symétriques.

Exercices.

1. Exprimer à l'aide des polynômes symétriques élémentaires de X_1, X_2, X_3, X_4 , les fractions rationnelles symétriques suivantes :

$$\Sigma X_1^2 X_2; \quad \Sigma \frac{X_1}{X_2}; \quad \Sigma \frac{1}{X_1}; \quad \prod_{i < j} (X_i + X_j).$$

2. Exprimer

$$\Delta = (a - b)^2(a - c)^2(b - c)^2$$

à l'aide des fonctions symétriques élémentaires de a, b, c .

En déduire la valeur de Δ (appelée discriminant de l'équation) quand a, b, c sont les racines de

$$X^3 + pX + q$$

puis de

$$X^3 + a_1X^2 + a_2X + a_3.$$

3. Écrire la condition nécessaire et suffisante entre les nombres complexes p et q pour que l'une des racines de $X^3 + pX + q$ ait un carré égal à la somme des carrés des deux autres.

4. Calculer l'aire du triangle défini par les nombres complexes racines de

$$X^3 + pX + q \in \mathbb{C}[X]$$

ainsi que le rayon du cercle circonscrit.

5. En appelant S_p le polynôme symétrique ΣX_i^p des n indéterminées, montrer l'égalité

$$S_p = S_{p-1}\sigma_1 - \sum_{i \neq j} X_i^{p-1} X_j$$

En déduire, pour $p \leq n$ et $p > n$ respectivement, les formules de Newton

$$S_p = S_{p-1}\sigma_1 - S_{p-2}\sigma_2 + \cdots + (-1)^{p-2} S_1\sigma_{p-1} + (-1)^{p-1} p\sigma_p$$

$$S_p = S_{p-1}\sigma_1 - S_{p-2}\sigma_2 + \cdots + (-1)^{n-2} S_{p-n+1}\sigma_{n-1} + (-1)^{n-1} S_{p-n}\sigma_n$$

(les σ_i sont comme toujours les polynômes symétriques élémentaires).

6. Si n éléments sont algébriquement indépendants sur K , il en est de même de leurs n fonctions symétriques élémentaires.

Transformer une équation

Substitutions.

Si f est une fraction rationnelle à une indéterminée sur le corps K , la **substitution** de f dans le polynôme $P \in K[X]$ donne une fraction rationnelle, notée $P \circ f$.

Si l'on écrit

$$P = a_0 + a_1X + \cdots + a_nX^n$$

on obtient

$$P \circ f = a_0 + a_1f + \cdots + a_nf^n$$

et l'on dit que l'équation

$$a_0 + a_1f(Y) + \cdots + a_nf^n(Y) = 0$$

est la **transformée** de l'équation

$$a_0 + a_1X + \cdots + a_nX^n = 0$$

par la substitution $X = f(Y)$. En la multipliant par le dénominateur de $f^n(Y)$, on trouve bien une équation algébrique, mais son degré sera en général supérieur à n : en effet, à toute racine α de l'équation $P(X) = 0$ correspondent *toutes* les racines de l'équation $f(Y) - \alpha = 0$.

En fait, il se pourra que l'équation transformée soit plus « simple » que celle de départ (par exemple, si elle est puissance d'une équation de degré inférieur).

Le cas le plus élémentaire de substitution est donné par les **translations**. Si l'on substitue X par $Y + u$, où u est dans le corps K , le degré ne change pas, et il reste

$$P(Y + u) = a_n(Y + u)^n + a_{n-1}(Y + u)^{n-1} + \cdots + a_1(Y + u) + a_0.$$

Le coefficient dominant est toujours a_n (supposé non nul), celui de Y^{n-1} est

$$na_n + a_{n-1}.$$

Si n est non nul dans K (en particulier si K contient $\mathbb{Q}$), le « bon choix » est

$$u = -\frac{a_{n-1}}{na_n}.$$

On a montré :

Par une translation adéquate, on peut annuler le coefficient précédant le dominant.

Une autre substitution classique, $Y = \frac{1}{X}$, sera vue au paragraphe suivant.

Cette idée d'assez naturelle

En partant d'une fraction : polynôme de c

On peut le $f(x_i)$ qui sont

coefficients de groupements f

En posant transformée de

Une remarque

pour une fraction de degré 1, on ne

Quelques ex

avec $a_n \neq 0$.

• Équation

La transform

et, au lieu de simple d'écrire

Transformations d'ordre un d'une équation.

Le polynôme

$$X^2 + aX + b$$

a pour racines (x_1, x_2) . Quel est le polynôme de degré 2 ayant pour racines (x_1^2, x_2^2) ?

On peut calculer les fonctions symétriques élémentaires

$$\begin{aligned} x_1^2 + x_2^2 &= (x_1 + x_2)^2 - 2x_1x_2 = a^2 - 2b \\ x_1^2x_2^2 &= (x_1x_2)^2 = b^2 \end{aligned}$$

d'où le polynôme cherché

$$X^2 - (a^2 - 2b)X + b^2.$$

Cette idée de « transformer » une équation par une fonction rationnelle est assez naturelle et peut parfois mener à une équation plus simple.

En partant d'un polynôme $P \in K[X]$ de degré n , de racines $(x_1, \dots, x_n)$, et d'une fraction rationnelle $f \in K(X)$, il existe un unique (à un facteur constant près) polynôme de degré n dont les racines sont $(f(x_1), \dots, f(x_n))$.

On peut le calculer, soit à l'aide des fonctions symétriques élémentaires des $f(x_i)$ qui sont des fonctions symétriques des x_i , donc s'expriment à l'aide des coefficients de P , soit encore en « bricolant » pour faire apparaître des groupements $f(X)$ dans l'équation $P(X) = 0$.

En posant $Y = f(X)$, l'équation $Q(Y) = 0$ obtenue s'appelle équation transformée de la première par f .

Une remarque : si $Y = f(X)$ s'écrit

$$X = g(Y)$$

pour une fraction rationnelle g , c'est-à-dire si f est quotient de polynômes de degré 1, on ne fait que substituer X par $g(Y)$.

Quelques exemples classiques, en partant de

$$P = a_0 + a_1X + \dots + a_nX^n$$

avec $a_n \neq 0$.

- Équation aux inverses.

La transformation est ici

$$Y = \frac{1}{X}$$

et, au lieu de calculer les fonctions symétriques élémentaires des $\frac{1}{x_i}$, il est plus simple d'écrire $P(X) = 0$ sous la forme

$$\frac{1}{X^n} P(X) = 0$$

une équation

sur le corps K , la
fraction rationnelle,

0

numérateur de $f^n(Y)$, on
a en général supérieur à
correspondent toutes les

is « simple » que celle de
on de degré inférieur).

tr les translations. Si l'on
ne change pas, et il reste

+ $a_1(Y + u) + a_0$.

1 nul), celui de Y^{n-1} est

$\mathbb{Q}$), le « bon choix » est

annuler le coefficient

u paragraphe suivant.

d'où, en remplaçant $\frac{1}{X}$ par Y , l'équation aux inverses

$$a_n + a_{n-1}Y + a_{n-2}Y^2 + \dots + a_1Y^{n-1} + a_0Y^n = 0.$$

Le polynôme du premier membre s'appelle **polynôme réciproque** de P , il est égal à $X^n P\left(\frac{1}{X}\right)$, où n est le degré de P ; *a posteriori*, ses coefficients donnent les fonctions symétriques élémentaires des inverses des racines de P . Cette équation n'est bien sûr autre que la substitution de X par $\frac{1}{Y}$ dans l'équation $P(X) = 0$.

Ainsi le polynôme réciproque de $X^3 + pX + q$ est

$$qX^3 + pX^2 + 1.$$

Si (x_1, x_2, x_3) sont les racines de P , on en déduit directement

$$\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} = -\frac{p}{q}$$

(bien sûr, q est supposé non nul pour que 0 ne soit pas racine du polynôme de départ).

• *Équation aux carrés.*

On s'intéresse à la transformation $Y = X^2$, et ici encore il y a une méthode plus rapide que celle consistant à calculer les fonctions symétriques élémentaires des x_i^2 . Le polynôme $P(X)$ s'écrit de manière unique

$$XA(X^2) + B(X^2)$$

en groupant les exposants pairs et les exposants impairs. L'équation $P(X) = 0$ se met alors sous la forme

$$XA(X^2) = -B(X^2), \quad \text{ou} \quad XA(Y) = -B(Y),$$

d'où, en élevant au carré,

$$X^2 A^2(Y) = B^2(Y)$$

ce qui donne l'équation transformée

$$YA^2(Y) - B^2(Y) = 0.$$

En effet, le polynôme du premier membre a même degré que P (pourquoi ?) et, si x est racine de P , son carré x^2 est racine de ce premier membre (pourquoi ?); c'est donc, pour raisons d'unicité, le polynôme cherché.

Pour calculer l'équation aux carrés de $X^3 + pX + q$, on écrit

$$X(X^2 + p) = -q$$

d'où

$$Y(Y + p)^2 - q^2 = 0.$$

Un cas,
nuls (c'est

Dans ce
l'équation

se réduit à

Si x est
aux carrés
Bien en
en itérant.

En fait,
 X entre le

(si f est un
par le dén
L'équat
en X , et c

L'équation aux carrés est

$$Y^3 + 2pY^2 + p^2Y - q^2 = 0.$$

On en déduit par exemple

$$x_1^2 + x_2^2 + x_3^2 = -2p$$

ce que l'on aurait pu retrouver à l'aide des fonctions symétriques élémentaires des x_i

$$x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3) = -2p.$$

Un cas particulier : celui où les coefficients de degré impair dans P sont tous nuls (c'est-à-dire $A = 0$).

Dans ces conditions $P(X)$ s'écrit $Q(X^2)$ pour un polynôme Q de degré $\frac{n}{2}$, et l'équation aux carrés, que l'on trouve égale à

$$Q^2(Y) = 0$$

se réduit bien sûr à

$$Q(Y) = 0.$$

Si x est racine simple de P , il est clair que x^2 sera racine double de l'équation aux carrés car $-x$ est aussi racine de P .

Bien entendu, l'équation aux puissances quatrièmes, huitièmes, etc. s'obtient en itérant.

On a calculé ci-dessus la somme des puissances quatrièmes des racines de $X^3 - 2X^2 + 1$. Retrouvons-la.

L'équation aux carrés s'obtient en écrivant $Y = X^2$ et

$$YX = 2Y - 1$$

d'où

$$Y^3 = (2Y - 1)^2$$

$$Y(Y^2 + 4) = 4Y^2 + 1.$$

Si l'on pose maintenant $Y^2 = Z$ et que l'on élève au carré, le résultat cherché est l'opposé du coefficient de Z^2 dans

$$Z(Z + 4)^2 - (4Z + 1)^2.$$

On tombe bien sur 8.

En fait, transformer $P(X) = 0$ par $Y = f(X)$ signifie tout simplement éliminer X entre les deux équations

$$\begin{cases} P(X) = 0 \\ f(X) - Y = 0 \end{cases}$$

(si f est un polynôme ; dans le cas où f est une fraction rationnelle, on multiplie par le dénominateur).

L'équation transformée n'est donc autre que le résultant de ces deux équations en X , et c'est bien un polynôme en Y .

Transformations d'ordre supérieur : notion de conjugués.

- Si (x_1, x_2) sont les racines de

$$X^2 + aX + b$$

cherchons maintenant une équation ayant pour racine $x_1 - x_2$. Comme x_1 et x_2 ne sont pas « différenciées », il y aura aussi la racine $x_2 - x_1$. La somme des deux est nulle, le produit vaut

$$\begin{aligned}(x_1 - x_2)(x_2 - x_1) &= -(x_1 - x_2)^2 \\ &= -(x_1 + x_2)^2 + 4x_1x_2 \\ &= -a^2 + 4b.\end{aligned}$$

L'équation cherchée est donc

$$X^2 + a^2 - 4b = 0.$$

- Partons maintenant des racines (x_1, x_2, x_3) de

$$X^3 + pX + q.$$

Si l'on veut avoir $x_1 - x_2$ pour racine d'une équation sans changer le corps des coefficients, on devra encore, *a priori*, avoir $x_2 - x_1$, mais aussi $x_1 - x_3$, $x_2 - x_3$, et leurs opposés. On tombera sur une équation de degré 6, mais qui sera en fait de degré 3 en X^2 car toute racine s'accompagne de son opposée. Il vaut donc mieux poser

$$y = (x_1 - x_2)^2$$

et chercher l'équation de degré 3 ayant pour racines

$$(x_1 - x_2)^2, \quad (x_2 - x_3)^2 \quad \text{et} \quad (x_1 - x_3)^2.$$

Écrivons

$$(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = x_3^2 + \frac{4q}{x_3}$$

en tenant compte des égalités

$$x_1 + x_2 + x_3 = 0 \quad \text{et} \quad x_1x_2x_3 = -q.$$

Mais x_3^3 est égal à $-px_3 - q$, d'où

$$(x_1 - x_2)^2 = \frac{x_3^3 + 4q}{x_3} = -p + \frac{3q}{x_3}$$

ce qui montre que notre équation cherchée, de racine $(x_1 - x_2)^2$, est la transformée de $P(X) = 0$ par $Y = -p + \frac{3q}{X}$. On substitue donc X par

$$\frac{3q}{Y + p}$$

Tout ceci
racines $(x_1,$
l'entier m é
s'obtiendra

un arrange

arrangemen
 $P(X) = 0$.

La suite c

et leurs fonc
donc s'expr
 $f(x_1, \dots, x_r$

d'où l'équation

$$\frac{27q^3}{(Y+p)^3} + \frac{3pq}{Y+p} + q = 0$$

ou encore

$$q(Y+p)^3 + 3pq(Y+p)^2 + 27q^3 = 0$$

$$(Y+p)^3 + 3p(Y+p)^2 + 27q^2 = 0.$$

En développant, on trouve

$$Y^3 + 6pY^2 + 9p^2Y + 4p^3 + 27q^2 = 0.$$

Le polynôme de degré 6 ayant pour racine la différence de deux racines arbitraires de $X^3 + pX + q$ est donc finalement

$$X^6 + 6pX^4 + 9p^2X^2 + 4p^3 + 27q^2.$$

On retrouve en particulier : le polynôme $X^3 + pX + q$ a une racine multiple si, et seulement si,

$$4p^3 + 27q^2$$

est nul (car alors 0 est racine du polynôme transformé). Ce résultat avait été démontré par d'autres moyens.

• Ainsi la famille des racines de $X^3 - X$ est (0, 1, -1), la famille des carrés des différences deux à deux est (1, 1, 4), d'où l'équation

$$(Y-1)^2(Y-4) = 0.$$

On retrouve bien l'équation ci-dessus, p étant égal à -1 et q à 0.

Tout ceci se généralise aisément. On part de $P \in K[X]$, de degré n , de ses racines $(x_1, \dots, x_n)$, et d'une fraction rationnelle f à m indéterminées sur K , l'entier m étant inférieur à n . Une équation ayant pour racine $f(x_1, \dots, x_m)$ s'obtiendra en adjoignant comme racines tous les $f(x_{i_1}, \dots, x_{i_m})$ où $(i_1, \dots, i_m)$ est un arrangement m à m . Il y a $\frac{n!}{(n-m)!}$ tels arrangements, et les valeurs de f sur ces arrangements s'appellent les **conjugués** de $f(x_1, \dots, x_m)$ par rapport à l'équation $P(X) = 0$.

La suite des conjugués est de longueur

$$\frac{n!}{(n-m)!}$$

et leurs fonctions symétriques élémentaires sont des fonctions symétriques des x_i , donc s'expriment rationnellement à l'aide des coefficients de P . On trouve ainsi $f(x_1, \dots, x_m)$ comme racine d'une équation de degré

$$\frac{n!}{(n-m)!} = n(n-1) \dots (n-m+1)$$

pour racine $x_1 - x_2$.
es », il y aura aussi la
ulle, le produit vaut

$$\binom{2}{2}^2 + 4x_1x_2$$

x_3) de

d'une équation sans
encore, *a priori*, avoir
et leurs opposés. On
ais qui sera en fait de
gne de son opposée. Il

pour racines

$$(x_1 - x_3)^2.$$

$$x_2 = x_3^2 + \frac{4q}{x_3}$$

$$x_2x_3 = -q.$$

$$-p + \frac{3q}{x_3}$$

e, de racine $(x_1 - x_2)^2$,

$$-p + \frac{3q}{X}. \text{ On substitue}$$

que l'on appelle transformée de $P(X) = 0$ par

$$Y = f(X_1, \dots, X_m).$$

A priori, on ne voit pas l'intérêt, vu que ce degré est supérieur à n .

Mais il peut arriver que les conjugués de $f(x_1, \dots, x_m)$ soient « assez » liés les uns aux autres.

Ainsi, si chacun se répète q fois, le polynôme en Y est puissance $q^{\text{ième}}$ d'un polynôme de degré $\frac{n!}{(n-m)!q}$, donc l'équation en Y se ramène à une équation de degré $\frac{n!}{(n-m)!q}$ et cet entier peut être inférieur à n .

De même, il se peut que les conjugués soient deux à deux opposés, auquel cas l'équation en Y est une équation de degré moitié en $Z = Y^2$. De toutes façons, il faudra beaucoup de « bicyclage » à la fois pour un choix intéressant de f et pour le calcul de l'équation en Y .

On retiendra en tout cas que le nombre de conjugués distincts donne le degré d'une équation, à coefficients dans le corps de base, vérifiée par $f(x_1, \dots, x_m)$.

Quelques exemples.

- Le cas $m = 1$ correspond à la transformée de $P(X) = 0$ par $Y = f(X)$. Les conjugués de $f(x_1)$ forment la suite

$$(f(x_1), f(x_2), \dots, f(x_n)).$$

- On a étudié, sur des cas particuliers, l'exemple de

$$f(X_1, X_2) = X_1 - X_2.$$

Au degré n , il y a $n(n-1)$ différences de couples de racines, donc la suite des conjugués de $x_1 - x_2$ est de longueur $n(n-1)$, chaque élément apparaissant avec son opposé. L'équation transformée de $P(X) = 0$ par $Y = X_1 - X_2$ sera de degré $n(n-1)$ en Y , mais de degré $\frac{n(n-1)}{2}$ en Y^2 .

Le terme constant de cette équation est, au signe près, égal à

$$\prod_{i < j} (x_i - x_j)^2$$

et sa nullité correspond exactement à l'existence d'une racine multiple de P . D'où son importance, sur laquelle on reviendra.

- Si l'on prend $X_1 + X_2$ au lieu de $X_1 - X_2$, on trouve, dans la suite des $n(n-1)$ conjugués de $x_1 + x_2$, chacun répété deux fois, donc on peut ramener l'équation transformée de $P(X) = 0$ par $Y = X_1 + X_2$ en une de degré

$$\frac{n(n-1)}{2}.$$

Une remarque

En particulier
 $\alpha = f(x_1, \dots, x_m)$
 sous-group

Pour faire le calcul explicite dans le cas

$$P = X^3 + aX^2 + bX + c$$

il serait maladroit de calculer les conjugués de $x_1 + x_2$ et leurs fonctions symétriques élémentaires, sans remarquer que $x_1 + x_2$ est égal à $-a - x_3$. Or l'équation transformée de P par $Y = -a - X$ est

$$\begin{aligned} (-Y - a)^3 + a(-Y - a)^2 + b(-Y - a) + c &= 0 \\ Y^3 + 2aY^2 + (a^2 + b)Y + ab - c &= 0. \end{aligned}$$

Ainsi, P aura deux racines opposées si, et seulement si, ab est égal à c . En réalité, la suite des conjugués de $x_1 + x_2$ est de longueur 6, et l'équation transformée de P par $X_1 + X_2$ est le carré de cette dernière; elle se réduit évidemment à cette équation de degré 3.

• Dans le cas $m = n$, les conjugués de $f(x_1, \dots, x_n)$ sont les $f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$ quand σ décrit le groupe Σ_n des permutations de n éléments.

L'équation en Y est de degré $n!$, mais ce degré peut d'autant plus être abaissé qu'il existe des permutations σ vérifiant

$$f(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)}).$$

On voit ici poindre l'importance que prendra le groupe des permutations des racines du polynôme.

Bien entendu, s'il y a « trop » de telles permutations, f n'a aucun intérêt, le cas caricatural étant celui où f est symétrique : l'équation en Y est alors puissance $(n!)$ d'une équation de degré 1. Ainsi, si f est la somme, la transformée de

$$a_0 + a_1X + \dots + a_nX^n = 0$$

par $Y = X_1 + \dots + X_n$ est

$$\left(Y + \frac{a_{n-1}}{a_n} \right)^{(n!)} = 0$$

qui se ramène à

$$Y + \frac{a_{n-1}}{a_n} = 0$$

et n'a aucun intérêt...

Une remarque.

En particulier, supposons qu'une certaine fonction rationnelle des racines, soit $\alpha = f(x_1, \dots, x_n)$, ne change pas quand on lui applique les éléments d'un certain sous-groupe H du groupe Σ_n de toutes les permutations.

Appelons p le nombre d'éléments de H , et remarquons que, si l'on applique $s \in \Sigma_n$ ou $sh \in \Sigma_n$ avec h dans H , on obtiendra le même résultat. Dès lors, le nombre de valeurs distinctes

$$f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$$

quand σ décrit Σ_n sera inférieur à $\frac{n!}{p}$, et α sera racine d'une équation de degré inférieur à $\frac{n!}{p}$ sur le corps de base K .

Le cas le plus simple est celui où H est cyclique, c'est-à-dire formé des puissances d'un élément $t \in \Sigma_n$.

Si $f(x_1, \dots, x_n)$ est égal à $f(x_{t(1)}, \dots, x_{t(n)})$, alors l'expression ne change pas si l'on applique les puissances de t , et leur nombre est l'ordre de t , ou plus petit entier $p > 0$ tel que t^p soit l'identité.

Un exemple que l'on rencontrera plus loin est celui de la **résolvante de Lagrange**

$$\alpha = x_1 + \omega x_2 + \dots + \omega^{n-1} x_n$$

où ω est une racine n -ième de l'unité.

Si l'on applique le cycle $\sigma = (1, 2, \dots, n)$, qui transforme chaque indice en le suivant et n en 1, α devient

$$\beta = x_2 + \omega x_3 + \dots + \omega^{n-2} x_n + \omega^{n-1} x_1 = \omega^{-1} \alpha$$

donc α^n ne change pas.

Comme σ est d'ordre n , on en déduit que la résolvante de Lagrange est racine n -ième d'une racine d'une équation de degré inférieur à

$$\frac{n!}{n} = (n-1)!$$

Exercices.

1. Transformer $X^3 + pX + q$ par

$$Y = \frac{1}{X^2}, \quad Y = X^3.$$

Étudier aussi les transformations d'ordre supérieur

$$Y = \frac{X_1}{X_2}, \quad Y = \frac{X_1}{X_2} + \frac{X_2}{X_3} + \frac{X_3}{X_1} \quad \text{et} \quad Y = X_1 + jX_2 + j^2X_3$$

(où j est une racine cubique non réelle de l'unité).

2. Écrire les équations aux carrés et aux cubes de

$$1 + X + X^2 + X^3 + X^4.$$

Effec

Mêm

3. Donr

4. A qu

a-t-il

On u
entre
polyr

si l'on applique
at. Dès lors, le

Effectuer aussi les transformations

$$Y = X - 1 \quad \text{et} \quad Y = X_1 + X_2.$$

Mêmes questions pour le polynôme

$$X^5 - 1.$$

3. Donner des équations égales à leur équation aux carrés.

4. A quelle condition sur $\alpha \in \mathbb{C}$ le polynôme

$$X^4 - \alpha X^3 - X^2 + 2$$

a-t-il deux racines inverses l'une de l'autre ?

On utilisera la méthode « directe », en adjoignant l'égalité $x_1 x_2 = 1$ aux relations entre coefficients et racines ; on traduira aussi la condition en éliminant X entre le polynôme et son polynôme réciproque.

ation de degré

dire formé des

ne change pas si
t, ou plus petit

est celui de la

ansforme chaque

$$\kappa_1 = \omega^{-1} \alpha$$

la résolvante de
équation de degré

$$+ jX_2 + j^2 X_3$$

Les équations de degré 3

La résolution d'une équation de degré 2 ne pose aucun problème : les racines de $X^2 + aX + b$ sont dans le corps engendré par les coefficients et une racine carrée de $a^2 - 4b$.

Passons donc au degré 3. Par une translation convenable, on a vu que l'on pouvait annuler le coefficient de degré 2. Et pour se placer dans le cadre le plus général, on va donc étudier l'équation

$$X^3 + pX + q = 0$$

où p et q sont des « lettres », c'est-à-dire algébriquement indépendants sur le corps $\mathbb{Q}$. Notre corps de base est donc le corps $\mathbb{Q}(p, q)$ des fractions rationnelles à deux indéterminées sur $\mathbb{Q}$ et tout cas « concret » se déduira de celui-ci, en remplaçant les lettres p et q par leurs valeurs dans les formules. La seule « restriction » concernant les corps est qu'ils contiennent tous $\mathbb{Q}$.

On appellera donc K ce corps $\mathbb{Q}(p, q)$, P le polynôme $X^3 + pX + q$, et (a, b, c) ses racines qui sont dans le corps de rupture de P sur K . Le but de ce paragraphe est de montrer que ces racines s'expriment algébriquement à l'aide de p et q , c'est-à-dire que toute équation de degré 3 est résoluble.

Génération du corps de rupture.

Avant d'aborder la résolution, examinons un moment le corps de rupture engendré par K et les racines a, b, c .

Ces racines sont caractérisées par les trois relations :

$$\begin{aligned} a + b + c &= 0 \\ ab + bc + ac &= p \\ abc &= -q. \end{aligned}$$

Il est clair que tout corps contenant a et b contient c : le corps de rupture est engendré par K et deux racines.

Mais si l'on connaît une racine a , on connaît la somme des deux autres, donc il suffit de connaître leur différence. Revoyons un calcul déjà fait :

$$\begin{aligned} (b - c)^2 &= (b + c)^2 - 4bc = a^2 + \frac{4q}{a} = \frac{a^3 + 4q}{a} \\ &= \frac{-pa + 3q}{a} = -p + 3(-a^2 - p) \end{aligned}$$

LES EQUATIONS

d'où finalement

Tout corps co
corps de ruptur

I
c

Une remarqu
de p et q nous pr
d'un dénominate
nullité de a entra
 $q = 0$.

Le discriminant.

Une autre cor
 p et q ne sont p
 $b - c$ est nulle

(le cas $q = 0$ exi
retrouve le résu

$$X^3 + pX$$

En fait, c'est

que l'on appelle

Il ne sera pa
expression $4p^3$
générale, ce qui
simples.

Le choix d'une

La résolution
se ramener soit
équations de de

d'où finalement les égalités :

$$(b - c)^2 = -3a^2 - 4p$$

$$a = \frac{3q}{(b - c)^2 + p}$$

Tout corps contenant a contient $(b - c)^2$, et réciproquement. En particulier, le corps de rupture est engendré par K et $(b - c)$.

Le corps de rupture d'une équation de degré 3 est engendré par le corps de base et la différence de deux racines.

Une remarque : dans le cas de l'équation générale, l'indépendance algébrique de p et q nous permet toutes les divisions ci-dessus sans scrupules, car la nullité d'un dénominateur entraînerait une relation de dépendance entre p et q . Ainsi, la nullité de a entraînerait la relation $q = 0$, celle de $(b - c)^2 + p$ entraînerait aussi $q = 0$.

Le discriminant.

Une autre conséquence du calcul concerne le cas d'une équation arbitraire (où p et q ne sont pas nécessairement algébriquement indépendants) : la différence $b - c$ est nulle si, et seulement si, a est égal à $\frac{3q}{p}$, ce qui s'écrit alors

$$27 \frac{q^3}{p^3} + 3q + q = 0$$

$$4p^3 + 27q^2 = 0$$

(le cas $q = 0$ exige $p = 0$, et réciproquement, comme on le voit directement). On retrouve le résultat :

$$X^3 + pX + q \text{ possède une racine multiple} \Leftrightarrow 4p^3 + 27q^2 \text{ est nul.}$$

En fait, c'est l'opposé

$$\Delta = -4p^3 - 27q^2$$

que l'on appelle **discriminant** de l'équation.

Il ne sera pas étonnant de voir apparaître dans le calcul des racines cette expression $4p^3 + 27q^2$. Bien entendu, elle n'est pas nulle dans le cas de l'équation générale, ce qui correspond bien au fait qu'une telle équation n'a que des racines simples.

Le choix d'une transformation.

La résolution de l'équation générale va consister à *transformer* l'équation pour se ramener soit à des équations binômes (extractions de radicaux), soit à des équations de degrés strictement inférieurs.

On doit donc introduire astucieusement une certaine fonction rationnelle $f(a, b, c)$ des racines.

Une « simple » serait de la forme $f(a, b, c) = au + bv + cw$, pour certains u, v, w dans une extension du corps de base $K = \mathbb{Q}(p, q)$. On veut que le nombre de valeurs *distinctes* prises par f sur les permutations de a, b, c , c'est-à-dire le nombre de conjugués de $au + bv + cw$ par rapport à l'équation, soit assez faible, car ce nombre donnera le degré d'une équation vérifiée par $f(a, b, c)$. Bien entendu, il ne faut pas non plus qu'il soit « trop » faible, c'est-à-dire égal à un : ceci se passe si u, v, w sont égaux, on va donc exclure ce cas.

La famille des six conjugués de $au + bv + cw$ s'obtient comme toujours en effectuant sur les racines (a, b, c) les six permutations; il revient au même d'effectuer ces permutations sur (u, v, w) .

Or le groupe Σ_3 des permutations de trois éléments est formé de deux classes :

- les trois permutations paires (l'identité et les deux permutations circulaires, celles qui ne laissent fixe aucun élément) qui forment le groupe alterné A_3 ;
- les trois transpositions, que l'on obtient en prenant l'une d'elles et en la composant successivement avec les trois permutations paires.

Autrement dit, si l'on appelle τ la transposition qui échange v et w , on écrira

$$\Sigma_3 = A_3 \cup A_3\tau$$

et l'on obtiendra la famille des conjugués de $au + bv + cw$ en effectuant :

- les trois permutations paires de u, v, w dans $au + bv + cw$;
- les trois permutations paires de u, v, w dans $au + cv + bw$.

Il convient donc de choisir les éléments u, v, w de manière que les permutations paires de (u, v, w) se traduisent « simplement » sur la valeur de $au + bv + cw$ (et de $au + cv + bw$).

Or il existe un choix de (u, v, w) tel que toute permutation paire revient à multiplier la suite (u, v, w) par un même élément, ce qui se traduira par une multiplication de $au + bv + cw$ par cet élément.

Ce choix de (u, v, w) est $(1, j, j^2)$, suite des racines cubiques de l'unité dans $\mathbb{C}$; on rappelle que j désigne $-\frac{1}{2} + i\frac{\sqrt{3}}{2}$, et que j^2 est à la fois son carré, son conjugué, et son inverse. On vérifie dans ces conditions que les images de $(1, j, j^2)$ par les trois permutations paires

$$(1, j, j^2), (j, j^2, 1) \text{ et } (j^2, 1, j)$$

sont les produits respectifs de la suite $(1, j, j^2)$ par 1, par j , et par j^2 .

Certes, j n'est pas dans le corps de base $K = \mathbb{Q}(p, q)$, mais on passe de K à l'extension *par radicaux* K_1 , sous-corps de $\mathbb{C}(p, q)$ engendré par K et les racines carrées de -3 . On va noter

$$K_1 = \mathbb{Q}(p, q, \sqrt{-3})$$

ce corps.

La démonstration

Conformément

Les six conjugués

(on parle de la famille des conjugués, donnée, racines a

$$x_1 x_2 = (\dots)$$

soit finalement

Il saute aux yeux que les six conjugués

L'équation

sera alors Autrement dit

ces éléments que leur image dans K_1 . Le discriminant

il est dans le discriminant

extension par radicaux $\mathbb{C}(p, q)$ engendré par K et les racines carrées de -3 . On va donc

engendrée par une extension

rationnelle

La démarche théorique.

Conformément au discours précédent, on va introduire les deux éléments

$$x_1 = a + bj + cj^2 \quad \text{et} \quad x_2 = a + cj + bj^2.$$

Les six conjugués de x_1 sont distincts deux à deux, ce sont

$$x_1; \quad jx_1; \quad j^2x_1; \quad x_2; \quad jx_2; \quad j^2x_2$$

(on parle ici de conjugués non au sens complexe mais au sens de l'équation donnée, ce sont les transformés de $a + bj + cj^2$ par les six permutations des racines a, b, c). On notera en passant que le produit x_1x_2 vaut

$$\begin{aligned} x_1x_2 &= (a + bj + cj^2)(a + cj + bj^2) \\ &= (a^2 + b^2 + c^2) - (ab + ac + bc) = (a + b + c)^2 - 3(ab + ac + bc) \end{aligned}$$

soit finalement

$$x_1x_2 = -3p.$$

Il saute alors aux yeux que si, au lieu de x_1 , on prend son cube x_1^3 , la suite de ses six conjugués par rapport à l'équation sera

$$x_1^3; \quad x_1^3; \quad x_1^3; \quad x_2^3; \quad x_2^3; \quad x_2^3.$$

L'équation donnant x_1^3 , c'est-à-dire la transformée de

$$X^3 + pX + q \quad \text{par} \quad Y = (X_1 + jX_2 + j^2X_3)^3$$

sera alors le cube d'une équation de degré 2 à coefficients dans K .

Autrement dit, si l'on pose

$$y_1 = (a + bj + cj^2)^3 \quad \text{et} \quad y_2 = (a + cj + bj^2)^3$$

ces éléments sont les racines d'une équation de degré deux sur K , ce qui entraîne que leur somme et leur produit sont nécessairement dans K (et *a fortiori* dans K_1).

Le discriminant de cette équation du second degré est

$$d = (y_1 + y_2)^2 - 4y_1y_2$$

il est dans K , donc dans K_1 , et l'on va adjoindre à K_1 une racine carrée de ce discriminant, que l'on notera $\sqrt{d}$, ce qui nous amène à considérer le corps

$$K_2 = \mathbb{Q}(p, q, \sqrt{-3}, \sqrt{d})$$

extension par radicaux successifs du corps de base $K = \mathbb{Q}(p, q)$, et sous-corps de $\mathbb{C}(p, q)$ engendré par K , $\sqrt{-3}$, et $\sqrt{d}$.

Ce corps K_2 contient y_1 et y_2 . Or x_1 et x_2 sont des racines cubiques de y_1 et y_2 . On va donc envisager une nouvelle extension par radicaux, notée

$$K_3 = \mathbb{Q}(p, q, \sqrt{-3}, \sqrt{d}, \sqrt[3]{y_1})$$

engendrée par K_2 et une racine cubique de y_1 , que l'on notera $\sqrt[3]{y_1}$: c'est bien une extension par radicaux de K_2 , car y_1 est dans K_2 .

Cette extension contient x_1 , donc aussi x_2 (d'après l'égalité $x_1 x_2 = -3p$), et par suite elle contient les trois racines a, b, c , qui sont les solutions du système linéaire :

$$\begin{aligned} a + b + c &= 0 \\ a + bj + cj^2 &= x_1 \\ a + bj^2 + cj &= x_2 \end{aligned}$$

On a donc démontré l'existence d'une chaîne de corps

$$K = \mathbb{Q}(p, q) \subset K(\sqrt{-3}) \subset K(\sqrt{-3}, \sqrt{d}) \subset K(\sqrt{-3}, \sqrt{d}, \sqrt[3]{y_1})$$

chacun engendré par le précédent et un radical relatif au précédent, et telle que le dernier corps contient les racines du polynôme $X^3 + pX + q$ (tout cela peut être plongé, pour la tranquillité de l'esprit, dans la clôture algébrique de K , contenue dans la clôture algébrique de $\mathbb{C}(p, q)$).

Traduction :

Toute équation algébrique de degré 3 est résoluble.

En d'autres termes, les racines d'une équation algébrique de degré 3 s'expriment algébriquement à l'aide des coefficients.

Le calcul explicite.

En pratique, tout revient à calculer

$$x_1 = a + bj + cj^2 \quad \text{et} \quad x_2 = a + bj^2 + cj.$$

On a montré que la somme et le produit de leurs cubes sont dans le corps de base $K = \mathbb{Q}(p, q)$. Vérifions-le :

$$\begin{aligned} x_1^3 x_2^3 &= (-3p)^3 = -27p^3 \quad (\text{calcul déjà fait}) \\ x_1^3 + x_2^3 &= (x_1 + x_2)^3 - 3x_1 x_2 (x_1 + x_2) \\ &= (2a - b - c)^3 + 9p(2a - b - c) \\ &= (3a)^3 + 27pa \\ &= 27(a^3 + pa) \\ &= -27q. \end{aligned}$$

On a utilisé successivement la nullité de $1 + j + j^2$, la nullité de $a + b + c$ et le fait que a est racine de $X^3 + pX + q$.

Dans ces conditions, x_1^3 et x_2^3 sont racines de

$$X^2 + 27qX - 27p^3 \in K[X].$$

Donc x_1 et x_2 (et aussi leurs produits par j et j^2) sont racines de

$$X^6 + 27qX^3 - 27p^3 \in K[X].$$

Le discriminant du polynôme $X^2 + 27qX - 27p^3$ est

$$d = (27q)^2 + 4 \times 27p^3 = 27(4p^3 + 27q^2).$$

LES EQU

En app
que l'on a
les valeur

sont

- 27

On cho
autres éta
n'importe

En notant
toutefois i

Appelo
adéquates

Ce sont
n'a besoin

Un exemp

Prenons
racines do
Plaçons
 a, b, c de
 $\Delta = +32$
L'équati
ici

car p vaut
Son disc

$x_2 = -3p$, et
is du système

En appelant $\sqrt{4p^3 + 27q^2}$ une des racines carrées de $4p^3 + 27q^2$ (expression que l'on avait déjà rencontrée, égale à l'opposé du discriminant), on en déduit que les valeurs de

$$x_1^3 = (a + bj + cj^2)^3 \quad \text{et} \quad x_2^3 = (a + bj^2 + cj)^3$$

sont

$$\frac{-27q + \sqrt{27}\sqrt{4p^3 + 27q^2}}{2} \quad \text{et} \quad \frac{-27q - \sqrt{27}\sqrt{4p^3 + 27q^2}}{2}.$$

$(d, \sqrt[3]{y_1})$

et telle que le
cela peut être
de K , contenue

On choisit alors pour x_1 une racine cubique de la première expression (les autres étant les produits par j et j^2), mais alors pour x_2 on ne peut pas prendre n'importe laquelle des racines cubiques de la seconde, il faut prendre $x_2 = \frac{-3p}{x_1}$.

En notant par le symbole $\sqrt[3]{}$ ces deux racines cubiques (leur choix n'est pas toutefois indépendant l'une de l'autre) on trouve le système linéaire

$$\begin{aligned} a + b + c &= 0 \\ a + bj + cj^2 &= \sqrt[3]{\frac{-27q + \sqrt{27}\sqrt{4p^3 + 27q^2}}{2}} \\ a + bj^2 + cj &= \sqrt[3]{\frac{-27q - \sqrt{27}\sqrt{4p^3 + 27q^2}}{2}}. \end{aligned}$$

Appelons α la valeur choisie pour x_1 . Celle de x_2 est $\frac{-3p}{\alpha}$, et des combinaisons adéquates donnent pour a, b, c , racines de l'équation, les valeurs

$$\frac{1}{3}\left(\alpha - \frac{3p}{\alpha}\right), \quad \frac{1}{3}\left(j^2\alpha - j\frac{3p}{\alpha}\right) \quad \text{et} \quad \frac{1}{3}\left(j\alpha - j^2\frac{3p}{\alpha}\right).$$

Ce sont là les fameuses **formules de Cardan**. Inutile de préciser que personne n'a besoin de les retenir par cœur...

Un exemple.

Prenons par exemple le polynôme $X^3 - 2X + 1$. Le corps de base est ici $\mathbb{Q}$, les racines doivent donc s'exprimer à l'aide de radicaux de rationnels.

Plaçons-nous dans le corps des complexes, qui contient bien sûr les racines a, b, c de $X^3 - 2X + 1$. Elles sont simples car le discriminant $\Delta = +32 - 27 = 5$ est non nul.

L'équation dont sont racines $(a + bj + cj^2)^3 = y_1$ et $(a + bj^2 + cj)^3 = y_2$ est ici

$$X^2 + 27X + 8 \times 27$$

car p vaut -2 et q vaut 1 .

Son discriminant est $27(27 - 32) = -5 \times 27 = -15 \times 3^2$.

de degré 3

corps de base

$a + b + c$ et

de

En prenant $i\sqrt{15}$ comme racine carrée de -15 , on trouve pour y_1 et y_2 les valeurs

$$\frac{-27 + 3i\sqrt{15}}{2} \quad \text{et} \quad \frac{-27 - 3i\sqrt{15}}{2}$$

qui sont complexes conjuguées (ici, « conjugué » a son sens usuel dans $\mathbb{C}$).

Appelons $x_1 = \sqrt[3]{\frac{-27 + 3i\sqrt{15}}{2}}$ une racine cubique de y_1 . Le produit $x_1 x_2$ étant réel (égal à $-3p = 6$) on doit prendre pour x_2 le complexe conjugué de x_1 (car y_2 est égal à $\overline{y_1}$, et x_2 est une racine cubique de $\overline{y_1}$ dont le produit avec x_1 est réel, c'est donc $\overline{x_1}$).

Le système

$$\begin{aligned} a + b + c &= 0 \\ a + bj + cj^2 &= x_1 \\ a + bj^2 + cj &= \overline{x_1} \end{aligned}$$

donne pour a, b, c les valeurs

$$\frac{1}{3}(x_1 + \overline{x_1}), \quad \frac{1}{3}(j^2 x_1 + j \overline{x_1}) \quad \text{et} \quad \frac{1}{3}(j x_1 + j^2 \overline{x_1}).$$

Toutes les trois sont *réelles*, ce qui prouve que le corps de rupture est en fait contenu dans $\mathbb{R}$, donc que l'extension par radicaux successifs que l'on a utilisée ici, c'est-à-dire

$$\mathbb{Q}\left(i\sqrt{3}, i\sqrt{15}, \sqrt[3]{\frac{-27 + 3i\sqrt{15}}{2}}\right)$$

contient strictement le corps de rupture. Mais peu importe, les complexes non réels introduits, comme j ou $i\sqrt{15}$, disparaissent à la fin.

En appelant α une racine cubique complexe de $\frac{-27 + 3i\sqrt{15}}{2}$, les autres racines cubiques sont alors $j\alpha$ et $j^2\alpha$, et l'on trouve pour racines de $X^3 - 2X + 1$ les trois réels

$$\frac{2}{3}\operatorname{Re} \alpha, \quad \frac{2}{3}\operatorname{Re} j\alpha \quad \text{et} \quad \frac{2}{3}\operatorname{Re} j^2\alpha$$

où Re désigne la partie réelle d'un complexe (demi-somme avec son conjugué complexe).

Le cas où les coefficients sont réels.

Une équation de degré 3 à coefficients réels peut avoir des racines toutes réelles (exemple ci-dessus) ou non (exemple de $X^3 - 1$, qui a une seule racine réelle).

LES ÉQUAT.

En fait, si l'

- si le con-
- complexe $\bar{\alpha}$;
- il existe t
- il y a une
- cas les racines

Autrement
une réelle et c

Comment d
tout dépend d
En conserva

- $\Delta < 0$. Al
- prendre x_1 et x
- ne le sont pas
- $\Delta > 0$. Al
- comme l'une a
- signalé ci-dessu
- $x_1 x_2$, égal à -
- degré 2 à coeffi
- de $j^2 x_1$ et $j x_2$, c
- racines sont ré

où α est une ra

Le dernier c.
paradoxe : po
coefficients *réel*
dans le corps d

La réponse c
donnant les ra
précisément, or
successifs du c
factorisable dar
« englober » le
(voir p. 244).

Exercices.

1. Pour l'équ

de racines :

En fait, si $P \in \mathbb{R}[X]$ est de degré 3, on vérifie facilement :

- si le complexe α est racine de P , il en est de même de son conjugué complexe $\bar{\alpha}$;
- il existe toujours au moins une racine réelle ;
- il y a une racine multiple si, et seulement si, le discriminant est nul, et en ce cas les racines sont toutes réelles.

Autrement dit, si les racines sont toutes simples, il y en a soit trois réelles, soit une réelle et deux non réelles complexes conjuguées.

Comment distinguer ces deux cas ? Pour $P = X^3 + pX + q$, on va voir que tout dépend du signe du discriminant $\Delta = -4p^3 - 27q^2$.

En conservant les notations de la démonstration, on va étudier les deux cas :

- $\Delta < 0$. Alors $4p^3 + 27q^2$ est positif, donc x_1^3 et x_2^3 sont réels et l'on peut prendre x_1 et x_2 réels, auquel cas $x_1 + x_2$ est réel, mais $j^2x_1 + jx_2$ et $jx_1 + j^2x_2$ ne le sont pas : il y a une racine réelle et deux non réelles complexes conjuguées ;
- $\Delta > 0$. Alors $4p^3 + 27q^2$ est négatif, donc x_1^3 et x_2^3 sont non réels. Mais comme l'une au moins des racines de $X^3 + pX + q$ est toujours réelle (on l'a signalé ci-dessus), on peut choisir x_1 et x_2 de manière que $x_1 + x_2$ soit réel. Or x_1x_2 , égal à $-3p$, est réel, donc x_1 et x_2 , non réels mais racines d'une équation de degré 2 à coefficients réels, sont complexes conjugués ; dès lors il en est de même de j^2x_1 et jx_2 d'une part, de jx_1 et j^2x_2 de l'autre, d'où il résulte que les trois racines sont réelles. Elles s'écrivent d'ailleurs

$$\frac{2}{3} \operatorname{Re} \alpha, \quad \frac{2}{3} \operatorname{Re} j\alpha, \quad \frac{2}{3} \operatorname{Re} j^2\alpha,$$

où α est une racine cubique de $\frac{-27q + i\sqrt{27}\sqrt{-4p^3 - 27q^2}}{2}$.

Le dernier cas (qui est celui de l'exemple ci-dessus) présente un apparent paradoxe : pourquoi, dans le calcul des racines *réelles* d'une équation à coefficients *réels*, faire intervenir des complexes non réels ? Ne peut-on pas rester dans le corps des réels ?

La réponse est négative : on montre qu'il n'existe aucune formule *réelle* donnant les racines d'une équation réelle de degré 3 à racines réelles. Plus précisément, on montre qu'il n'existe, dans $\mathbb{R}$, aucune extension par radicaux successifs du corps des coefficients telle que le polynôme soit totalement factorisable dans cette extension. Il faut obligatoirement passer dans $\mathbb{C}$ pour « englober » le corps de rupture à l'aide d'adjonctions successives de radicaux (voir p. 244).

Exercices.

1. Pour l'équation

$$X^3 + aX^2 + bX + c = 0$$

de racines x_1, x_2, x_3 , montrer que

$$(x_1 + x_2j + x_3j^2)^3$$

est racine de

$$X^2 + (2a^3 - 9ab + 27c)X + (a^2 - 3b)^3 = 0.$$

2. Résoudre $X^3 + pX + q = 0$ par l'artifice suivant : on pose $X = Y + Z$, où Y et Z sont liés par $3YZ + p = 0$.

Calculer Y^3 et Z^3 et retrouver les formules de Cardan.

3. Dans le calcul des racines de l'équation générale de degré 3, soit $X^3 + pX + q = 0$, montrer que, si a, b, c sont les racines et si l'on pose $x = a + bj + cj^2$, alors x vérifie

$$x^2 - 3ax - 3p = 0.$$

En déduire que $\frac{x}{3} - \frac{p}{x}$ est racine de

$$T = X^3 + pX + q.$$

Effectuer alors dans l'équation $T(X) = 0$ la substitution $X = \frac{Y}{3} - \frac{p}{Y}$ et montrer que l'on retrouve l'équation de degré 6 en Y (mais de degré 2 en Y^3) dont sont racines

$$a + bj + cj^2 \quad \text{et} \quad a + bj^2 + cj.$$

4. Calculer les racines de

$$X^3 + X^2 + 1, \quad X^3 + 2X + 1 \quad \text{et} \quad X^3 + X^2 + X + 1.$$

5. Si l'une des racines de $X^3 + pX + q$ est x , les deux autres sont

$$\frac{(d - 9q)x + 2p^2}{6px + 9q + d}$$

où d est successivement égal aux deux racines carrées de Δ .

Passons à
résolution de

où a, b, c sont
On va donc
indéterminée

s'expriment à
En remplaçant
contenant Q
résoluble.

Disons tout
prouvant que
p. 241).

Le groupe de

Appelons

Ces racines
on va chercher
de conjugués
permutations
intérêt : on se
Il est clair que
intervenir ici ;
sous-groupe »
Commençons
 $N = \{3, 4\}$. S
invariants, et
permutations

ou encore

+ Z, où Y et Z

degré 3, soit
si l'on pose

$\frac{p}{Y}$ et montrer
 Y^3) dont sont

X + 1.

Les équations de degré 4

Passons au degré 4. Par la translation habituelle, le problème revient à la résolution de l'équation

$$X^4 + aX^2 + bX + c = 0$$

où a, b, c sont algébriquement indépendants sur le corps $\mathbb{Q}$.

On va donc partir du corps $\mathbb{Q}(a, b, c)$ des fractions rationnelles à trois indéterminées sur $\mathbb{Q}$ et, ici encore, on va montrer que les racines de

$$X^4 + aX^2 + bX + c$$

s'expriment algébriquement à l'aide des coefficients.

En remplaçant ensuite a, b, c par des éléments de n'importe quel corps contenant $\mathbb{Q}$, on en déduira que toute équation algébrique de degré 4 est résoluble.

Disons tout de suite que l'on s'arrêtera au degré 4, un résultat plus difficile prouvant que l'équation générale de degré supérieur à 5 est non résoluble (voir p. 241).

Le groupe des permutations.

Appelons x_1, x_2, x_3, x_4 les racines de l'équation générale

$$X^4 + aX^2 + bX + c = 0.$$

Ces racines sont bien sûr dans le corps de rupture du polynôme et, ici encore, on va chercher une fonction rationnelle $f(x_1, x_2, x_3, x_4)$ des racines ayant « peu » de conjugués distincts, c'est-à-dire prenant « peu » de valeurs distinctes sur les 24 permutations des racines. Mais « peu » ne signifie pas « une seule », cas sans intérêt : on se gardera donc de prendre f symétrique.

Il est clair que la structure du groupe Σ_4 des permutations de quatre indices va intervenir ici ; on va effectuer ce que l'on appelle sa « partition modulo un certain sous-groupe ».

Commençons par grouper les indices en deux parties, en posant $M = \{1, 2\}$ et $N = \{3, 4\}$. Sur les 24 éléments de Σ_4 , il y en a quatre qui laissent M et N invariants, et quatre qui transforment la partie M en la partie N . Ces huit permutations forment un sous-groupe S de Σ_4 , qui contient par exemple

$$(1, 2, 3, 4) \rightarrow (2, 1, 3, 4)$$

ou encore

$$(1, 2, 3, 4) \rightarrow (4, 3, 1, 2)$$

mais ni

$$(1, 2, 3, 4) \rightarrow (1, 3, 2, 4)$$

ni

$$(1, 2, 3, 4) \rightarrow (3, 2, 1, 4).$$

Appelons par exemple σ cette dernière permutation, qui est hors de S ; la partie σS , formée de produits de σ par tous les éléments de S , possède huit éléments aussi (ce n'est bien sûr pas un sous-groupe!).

Il reste 8 éléments hors de $S \cup \sigma S$, par exemple

$$\tau : (1, 2, 3, 4) \rightarrow (4, 2, 3, 1).$$

En effet, il est clair que τ est hors de S , et il est hors de σS car $\sigma^{-1}\tau$ laisse fixe 2 et transforme 1 en 4, donc n'est pas dans S .

La partie τS est alors formée aussi de huit éléments et on vérifie sans peine que ces éléments sont hors de S et de σS .

On vient de réaliser une partition

$$\Sigma_4 = S \cup \sigma S \cup \tau S$$

en trois parties de huit éléments.

Dans ces conditions, toute fonction de quatre variables x_1, x_2, x_3, x_4 qui prend la même valeur sur les huit permutations appartenant à S prendra au plus trois valeurs distinctes en tout : sa valeur en (x_1, x_2, x_3, x_4) , sa valeur en $(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)})$ et sa valeur en $(x_{\tau(1)}, x_{\tau(2)}, x_{\tau(3)}, x_{\tau(4)})$.

Le choix d'une transformation.

Si l'on revient à la fonction rationnelle $f(x_1, x_2, x_3, x_4)$ cherchée, on la veut non symétrique, mais on veut qu'elle ne change pas si l'on effectue les huit permutations appartenant à S . L'idée la plus simple est de prendre

$$f(x_1, x_2, x_3, x_4) = \psi[\varphi(x_1, x_2), \varphi(x_3, x_4)]$$

où φ et ψ sont des fractions rationnelles symétriques à deux indéterminées, choisies de sorte que f ne soit pas symétrique.

Dans ces conditions $f(x_1, x_2, x_3, x_4)$ aura au plus trois conjugués distincts :

$$f(x_1, x_2, x_3, x_4), \quad f(x_3, x_2, x_1, x_4) \quad \text{et} \quad f(x_4, x_2, x_3, x_1)$$

donc sera racine d'une équation de degré 3 : on sait que cette dernière est résoluble. Restera ensuite à exprimer les x_i .

Le choix de Ferrari consiste à prendre la fonction produit pour φ et la fonction somme pour ψ .

Le calcul explicite

Posons donc $\alpha = x_1x_2 + x_3x_4$. Par rapport à l'équation, il a deux autres conjugués distincts, qui sont

$$\beta = x_3x_2 + x_1x_4 \quad \text{et} \quad \gamma = x_4x_2 + x_3x_1.$$

LES EQUA

Calculon

$$\alpha\beta\gamma = x_1$$

Dès lors.

D'après
algèbre
certaine ex

Les formul

Reste à r
l'aide de α
Il suffit r

On en dédu
et β . D'ail
trouve

Notons

On aura
de ces trois

$$(x_1 +$$

Comme
Finalem
 $\beta - \alpha$, not
ces deux r

Calculons donc les fonctions symétriques élémentaires de α, β, γ :

$$\alpha + \beta + \gamma = \sum_{i < j} x_i x_j = a.$$

$$\alpha\beta + \beta\gamma + \alpha\gamma = (\sum x_i) \left(\sum_{i < j < k} x_i x_j x_k \right) - 4x_1 x_2 x_3 x_4 = -4c.$$

$$\alpha\beta\gamma = x_1 x_2 x_3 x_4 (\sum x_i)^2 + \left(\sum_{i < j < k} x_i x_j x_k \right)^2 - 4x_1 x_2 x_3 x_4 \sum_{i < j} x_i x_j = b^2 - 4ac.$$

Dès lors, α, β, γ sont les trois racines du polynôme

$$X^3 - aX^2 - 4cX + 4ac - b^2.$$

D'après le chapitre précédent, ces trois racines α, β, γ s'expriment algébriquement à l'aide des coefficients, donc de a, b, c : elles sont dans une certaine extension par radicaux successifs du corps de base $\mathbb{Q}(a, b, c)$.

Les formules de Ferrari.

Reste à montrer que les racines x_1, x_2, x_3, x_4 s'expriment algébriquement à l'aide de α, β, γ .

Il suffit pour cela d'écrire les deux égalités

$$\begin{cases} (x_1 + x_3)(x_2 + x_4) = \alpha + \beta \\ (x_1 + x_3) + (x_2 + x_4) = 0. \end{cases}$$

On en déduit que $(x_1 + x_3)$ et $(x_2 + x_4)$ s'expriment algébriquement à l'aide de α et β . D'ailleurs, en appelant $\sqrt{-\alpha - \beta}$ une racine carrée de $-\alpha - \beta$, on trouve

$$\begin{aligned} x_1 + x_3 &= \sqrt{-\alpha - \beta} \\ x_2 + x_4 &= -\sqrt{-\alpha - \beta}. \end{aligned}$$

Notons en passant que $-\alpha - \beta$ est égal à $\gamma - a$.

On aura aussi besoin d'une racine carrée de $\beta - a$ et d'une de $\alpha - a$, le produit de ces trois racines carrées devant être égal à

$$(x_1 + x_2)(x_1 + x_4)(x_1 + x_3) = x_1^3 + x_1^2(x_2 + x_3 + x_4) + \sum_{i < j < k} x_i x_j x_k.$$

Comme $x_2 + x_3 + x_4$ vaut $-x_1$, il reste la dernière somme, égale à $-b$.

Finalement, on choisit une racine carrée de $\gamma - a$, notée $\sqrt{\gamma - a}$, une de $\beta - a$, notée $\sqrt{\beta - a}$; dans ces conditions le quotient de $-b$ par le produit de ces deux racines carrées est une racine carrée de $\alpha - a$, que l'on note $\sqrt{\alpha - a}$.

On écrit alors

$$\begin{aligned}x_1 + x_3 &= \sqrt{\gamma - a} \\x_2 + x_4 &= -\sqrt{\gamma - a} \\x_1 + x_4 &= \sqrt{\beta - a} \\x_2 + x_3 &= -\sqrt{\beta - a} \\x_1 + x_2 &= \sqrt{\alpha - a} \\x_3 + x_4 &= -\sqrt{\alpha - a}.\end{aligned}$$

En faisant des sommes adéquates, on trouve les expressions algébriques des x_i en fonction de a et des α, β, γ , qui, eux, s'expriment algébriquement à l'aide de a, b, c .

Ce sont les **formules de Ferrari**, qui s'écrivent :

$$\begin{aligned}2x_1 &= \sqrt{\gamma - a} + \sqrt{\beta - a} + \sqrt{\alpha - a} \\2x_2 &= -\sqrt{\gamma - a} - \sqrt{\beta - a} + \sqrt{\alpha - a} \\2x_3 &= \sqrt{\gamma - a} - \sqrt{\beta - a} - \sqrt{\alpha - a} \\2x_4 &= -\sqrt{\gamma - a} + \sqrt{\beta - a} - \sqrt{\alpha - a}.\end{aligned}$$

Ici encore, l'intérêt pratique de ces formules est limité (c'est le moins que l'on puisse dire...). Mais elles permettent d'affirmer :

Toute équation algébrique de degré 4 est résoluble.

Un exemple.

Prenons un exemple à peine truqué : si l'on veut que l'équation de degré 3 vérifiée par

$$x_1x_2 + x_3x_4 = \alpha$$

soit celle résolue au chapitre précédent, soit $X^3 - 2X + 1$, on doit prendre

$$a = 0; \quad c = \frac{1}{2}; \quad b^2 = -1.$$

On part donc de l'équation $X^4 + iX + \frac{1}{2} = 0$. Le corps engendré par les coefficients est ici $\mathbb{Q}(i)$, corps des complexes à coordonnées rationnelles.

Alors α et ses deux autres conjugués β et γ sont les racines de

$$X^3 - 2X + 1.$$

On a calc
ces racines

A partir c
des racines

$$\sqrt{6x_1} = \sqrt{\quad}$$

les radicaux
Les autre
carrées.
Inutile d'

Exercices

1. Résou

2. Le pol
 $b^2 - 4$

Utilise.

3. Montr
vérifian

En déd
écrire q
d'où de
degré 3

4. Les rac
cela ap
Explicit
deux ra

On a calculé ces racines : on choisit une racine cubique z de $\frac{-27 + 3i\sqrt{15}}{2}$, et ces racines sont

$$\frac{2}{3} \operatorname{Re} z, \quad \frac{2}{3} \operatorname{Re} jz \quad \text{et} \quad \frac{2}{3} \operatorname{Re} j^2 z.$$

A partir de ces valeurs de α, β, γ , et en tenant compte du fait que a est nul, l'une des racines de $X^4 + iX + \frac{1}{2}$ est alors donnée par

$$\sqrt{6}x_1 = \sqrt{\operatorname{Re} \sqrt[3]{\frac{-27 + 3i\sqrt{15}}{2}}} + \sqrt{\operatorname{Re} j \sqrt[3]{\frac{-27 + 3i\sqrt{15}}{2}}} + \sqrt{\operatorname{Re} j^2 \sqrt[3]{\frac{-27 + 3i\sqrt{15}}{2}}}$$

les radicaux étant choisis de manière adéquate.

Les autres s'obtiennent en variant les signes devant certaines des racines carrées.

Inutile d'insister sur le caractère inhumain de telles expressions...

Exercices

1. Résoudre l'équation générale de degré 4 à l'aide des transformations

$$y = (x_1 + x_2)(x_3 + x_4) \quad \text{et} \quad y = (x_1 + x_2 - x_3 - x_4)^2.$$

2. Le polynôme $X^4 + aX^2 + bX + c$ s'écrit $X^4 + (uX + v)^2$ si, et seulement si, $b^2 - 4ac$ est nul.

Utiliser cette remarque pour résoudre l'équation générale de degré 4.

3. Montrer qu'à l'aide d'une équation de degré 3 sur $\mathbb{Q}(a, b, c)$ on peut trouver u, v et w vérifiant

$$X^4 + aX^2 + bX + c = (X^2 + uX + v)(X^2 - uX + w).$$

En déduire une autre résolution de l'équation générale de degré 4. (On pourra écrire que le reste de la division euclidienne du polynôme par $X^2 + uX + v$ est nul, d'où deux équations entre lesquelles l'élimination de v conduit à une équation de degré 3 en u^2 .)

4. Les racines de $X^4 + aX^2 + c$ constituent deux couples de racines opposées. Où cela apparaît-il si l'on suit la démonstration générale, en tenant compte de $b = 0$? Expliciter les formules de Ferrari et retrouver les racines comme racines carrées des deux racines du polynôme

$$X^2 + aX + c.$$

5. Résoudre explicitement les équations suivantes :

$$X^4 + X + 1 = 0, \quad X^4 + X^3 - 1 = 0 \quad \text{et} \quad X^4 + X^3 + X^2 + X + 1 = 0.$$

6. Les racines de $X^4 + aX^3 + bX^2 + aX + 1$ sont données à l'aide d'extractions de racines carrées (autrement dit, ces racines sont constructibles à la règle et au compas). On pourra utiliser la transformation

$$Y = X + \frac{1}{X}.$$

Les ex
me » per
extension

On au
essentielle

Quant
aux sous-
contenant

caractéris

Rappel
élément n
noter $n1$.
présentent

• pour
définition
corps de F

• il exis
positif aya
l'intégrité

Dans c
caractérist
comme les

Dans le
caractérist

On note
générateur

Dans bie
à ceux qui c
le plus peti

$X + 1 = 0.$

extractions de
la règle et au

Les extensions de corps

Les exemples précédents montrent la nécessité de disposer d'un « mécanisme » permettant de passer d'un corps à un corps plus grand (c'est-à-dire une extension) à l'aide d'adjonctions d'un ou plusieurs éléments.

On aura besoin de notions très élémentaires d'espaces vectoriels : essentiellement ce qui concerne la définition de la dimension.

Quant à la théorie des corps, répétons que l'on pourra, le cas échéant, se borner aux sous-corps du corps $\mathbb{C}$ des complexes ou, plus généralement, à tout corps contenant $\mathbb{Q}$. Si l'on veut aller plus loin, on devra utiliser la notion de **caractéristique** d'un corps.

Rappelons-la brièvement. Pour tout corps K et tout entier $n \in \mathbb{N}$, on appelle élément n dans K la somme de n éléments égaux à 1. En toute rigueur, on doit le noter $n1$. On étend aux entiers négatifs en posant $n1 = -(-n)1$. Deux cas se présentent alors :

- pour tout $n \neq 0$, l'élément $n1$ de K est non nul ; il est alors inversible, d'où la définition de $r1$ pour tout $r \in \mathbb{Q}$, et l'ensemble de ces éléments forme un sous-corps de K isomorphe à $\mathbb{Q}$, c'est ce qui permet de dire « K contient $\mathbb{Q}$ » ;
- il existe $n \neq 0$ tel que $n1$ soit nul dans K ; le plus petit entier strictement positif ayant cette propriété est alors un nombre premier (évident grâce à l'intégrité de K) qui divise tous les autres.

Dans ce dernier cas, le nombre premier p en question s'appelle la caractéristique de K , et les opérations entre les éléments de la forme $n1$ se font comme les opérations entre entiers modulo p ; on dira alors « K contient $\mathbb{Z}/p$ ».

Dans le premier cas, la convention la plus usuelle est de dire que K est de caractéristique nulle.

On note $\text{car}K$ cette caractéristique, et en termes plus sophistiqués c'est le générateur de l'idéal noyau de l'homomorphisme

$$\begin{array}{l} n \rightarrow n1 \\ \mathbb{Z} \rightarrow K. \end{array}$$

Dans bien des cas on se bornera aux corps de caractéristique nulle, c'est-à-dire à ceux qui contiennent $\mathbb{Q}$. Le corps $\mathbb{Q}$ est alors le sous-corps engendré par 1, donc le plus petit sous-corps du corps donné : on l'appelle son sous-corps premier.

Bien entendu, si K est de caractéristique $p \neq 0$, le sous-corps premier de K est $\mathbb{Z}/p$. En toute rigueur, il faudrait dire que tout sous-corps premier est « isomorphe » à $\mathbb{Q}$ ou $\mathbb{Z}/p$, mais on fera l'identification sans aucun inconvénient.

Un corps fini est nécessairement de caractéristique non nulle, car il ne peut pas contenir $\mathbb{Q}$ qui est infini.

Enfin, comme dans tout ce livre, les corps seront toujours *commutatifs*.

Rappel
considère
des corps
Ainsi, t

Le degré.

On peu
plus d'une
En par
degré de 1

Une notati

Prenons
Il contient
dire les pol
l'ensemble

NS DE CORPS

premier de K est
ps premier est
n inconvénient.

se non nulle, car

ommutatifs.

Degré d'une extension

Rappelons qu'une **extension** d'un corps K est un *corps* contenant K ; on ne considérera pas les anneaux contenant K comme des extensions si ce ne sont pas des corps (exemple *ad hoc* de l'anneau $K[X]$ de polynômes).

Ainsi, tout corps est extension de son sous-corps premier, qui est $\mathbb{Q}$ ou $\mathbb{Z}/p$.

Le degré.

On peut voir une extension L de K comme un espace vectoriel sur K , muni en plus d'une multiplication qui en fait un corps et qui prolonge celle de K .

En particulier, L possède une dimension comme K -espace. On l'appelle le **degré** de L sur K , et on le note $L : K$.

- On écrira ainsi $\mathbb{C} : \mathbb{R} = 2$, une base de $\mathbb{C}$ sur $\mathbb{R}$ étant formée par exemple de 1 et i .
- Les corps $\mathbb{C}$ et $\mathbb{R}$ sont de degré infini sur $\mathbb{Q}$.
- Pour tout corps K , le corps $K(X)$ des fractions rationnelles est de degré infini sur K ; la suite $(1, X, X^2, \dots)$ des puissances de l'indéterminée est en effet une famille infinie libre, puisqu'une combinaison K -linéaire de cette famille est un polynôme, et que le seul polynôme nul est celui dont tous les coefficients sont nuls.
- Bien entendu, K est la seule extension de degré 1 sur K .

$$[L : K] = 1 \Leftrightarrow L = K.$$

- Toute extension de degré fini d'un corps fini est un corps fini. Plus précisément, si K est fini et si L est une extension de degré fini, on vérifie l'égalité

$$(\text{card } L) = (\text{card } K)^{(L : K)}.$$

Une notation.

Prenons un élément α d'une extension de K . Quel est le corps engendré par K et α ? Il contient les puissances de α , ainsi que leurs combinaisons K -linéaires, c'est-à-dire les polynômes en α , donc aussi les quotients de tels polynômes, qui forment l'ensemble des fractions rationnelles en α .

Or, cet ensemble des $\frac{P(\alpha)}{Q(\alpha)}$, où P décrit l'ensemble des polynômes sur K , et Q décrit l'ensemble des polynômes sur K ne s'annulant pas en α , forme un corps. On dira que le corps engendré par K et α (ou engendré par α sur K) est l'ensemble des valeurs en α des fractions rationnelles définies en α ; il est logique de le noter $K(\alpha)$, par analogie avec la notation $K(X)$ qui désigne le corps des fractions rationnelles, puisque l'on substitue X par α (quand c'est possible...).

On écrira ainsi $\mathbb{C} = \mathbb{R}(i)$, ou encore $\mathbb{C} = \mathbb{R}(z)$ où z est tout nombre complexe non réel.

On a déjà utilisé la notation $\mathbb{Q}(i)$, corps des nombres complexes à parties réelle et imaginaire rationnelles.

Si α est dans le corps K , on écrira bien sûr $K(\alpha) = K$.

On définit plus généralement l'extension $K(\alpha_1, \dots, \alpha_n)$ où les α_i sont dans une extension de K . On dira que c'est le corps engendré par les α_i sur K , ou encore que c'est le corps obtenu en adjoignant les α_i à K . Les éléments sont les valeurs en $(\alpha_1, \dots, \alpha_n)$ des fractions rationnelles à n indéterminées définies en ce point (c'est-à-dire pouvant s'écrire avec un dénominateur n'ayant pas $(\alpha_1, \dots, \alpha_n)$ pour racine).

On notera aussi que $K(\alpha_1, \dots, \alpha_n)$ n'est autre que $K(\alpha_1)(\alpha_2) \dots (\alpha_n)$: on peut adjoindre « un à un ».

On peut même adjoindre à K une partie Q , finie ou infinie, d'une extension et définir ainsi le corps $K(Q)$. Pour le déterminer, on pourra utiliser les fractions rationnelles. On pourra aussi voir pas à pas ce que l'on doit adjoindre quand on a déjà adjoint Q (les puissances, sommes, etc.) jusqu'à tomber sur un corps.

Si les σ_i sont les polynômes symétriques élémentaires de $X_1, \dots, X_n$ on a vu que $K(\sigma_1, \dots, \sigma_n)$ est le corps des fractions rationnelles symétriques en les X_i .

Un commentaire important.

Il convient de ne pas oublier qu'une écriture comme $K(\alpha)$ suppose que α est un élément d'une certaine extension L de K . Cette « grande » extension L n'aura plus de rôle ensuite, en dehors de son sous-corps engendré par K et α , mais elle est indispensable *a priori* pour la définition du corps $K(\alpha)$.

Ceci dit, on peut se passer de préciser dans quel « grand cadre » L on se place si l'ambiguïté n'est pas possible, ou si des conventions « usuelles » ne laissent pas de doute.

• Une notation comme $\mathbb{Q}(\sqrt{5})$ se passe de précisions : c'est le sous-corps de $\mathbb{C}$ engendré par une racine carrée de 5, car alors un tel corps contient aussi l'autre racine carrée, qui est son opposée. En général, on conserve la notation $\sqrt{5}$ pour désigner la seule racine carrée positive de 5, mais c'est une pure convention. Les éléments de $\mathbb{Q}(\sqrt{5})$ s'écrivent $a + b\sqrt{5}$, avec a et b dans $\mathbb{Q}$.

• Plus claire : c'est racine carrée. T l'autre de l'écriture ! comme l'

D'ailleu

• Tout possède d réelles qui

Dans ce $a + b\alpha +$ éléments s

avec $u, v,$

Ces de confondre

La raiso ne conten $\mathbb{Q}(j\alpha)$, ni $\mathbb{C}$

La con réelle, c'est

$\sqrt[3]{2}$ et $j\sqrt[3]{2}$ mais aussi

corps $\mathbb{Q}(\sqrt[3]{2})$ $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ précédente

• Ceci d $K(\sqrt[3]{x})$ n'a près, ce n'e l'on n'a pas de $X^3 - x$ l'unité, c'es possède un pour $\sqrt[3]{x}$, i

Les extensi

On pourr d'ailleurs de alors le deg

es sur K , et Q

un corps. On
l'ensemble des
le noter $K(\alpha)$,
s rationnelles,

où α est tout

s complexes à

$= K$.

α_i sont dans
 K , ou encore
les valeurs en
ce point (c'est-
... α_n) pour

... (α_n) : on

e extension et
r les fractions
re quand on a
un corps.

mentaires de
s des fractions

se que α est un
sion L n'aura
 α , mais elle est

on se place si
s » ne laissent

sous-corps de $\mathbb{C}$
it aussi l'autre
ation $\sqrt{5}$ pour
vention. Les

• Plus généralement, si x est dans le corps K , la notation $K(\sqrt{x})$ est aussi claire : c'est le sous-corps de la clôture algébrique de K engendré par K et une racine carrée de x dans cette clôture, ce sous-corps contient alors les deux racines carrées. Toutefois, il n'y a en général aucune convention particulierisant l'une ou l'autre de ces deux racines carrées opposées, et l'ambiguïté réside ici non dans l'écriture $K(\sqrt{x})$ mais dans l'élément $\sqrt{x}$, qu'il faudra fixer une fois pour toutes comme l'une des deux racines carrées si l'on veut travailler avec.

D'ailleurs, $K(\sqrt{x})$ est le corps de rupture sur K du polynôme $X^2 - x$.

• Tout ne marche pas aussi bien si l'on décrit par exemple $\mathbb{Q}(\sqrt[3]{2})$. En effet, $\mathbb{Q}$ possède dans $\mathbb{C}$ trois racines cubiques, une réelle que l'on notera α et deux non réelles qui sont $j\alpha$ et $j^2\alpha$.

Dans ces conditions, $\mathbb{Q}(\alpha)$ est un sous-corps de $\mathbb{R}$, formé des réels de la forme $a + b\alpha + c\alpha^2$, avec a, b, c dans $\mathbb{Q}$, alors que $\mathbb{Q}(j\alpha)$ n'est pas un sous-corps de $\mathbb{R}$, ses éléments sont les complexes de la forme

$$u + vj\alpha + wj^2\alpha^2$$

avec u, v, w dans $\mathbb{Q}$.

Ces deux corps sont bien isomorphes, mais on ne peut déceimment les confondre !

La raison, ici, est que le sous-corps de $\mathbb{C}$ engendré par une racine cubique de 2 ne contient pas toutes les racines cubiques de 2, ce qui signifie que ni $\mathbb{Q}(\alpha)$, ni $\mathbb{Q}(j\alpha)$, ni $\mathbb{Q}(j^2\alpha)$ ne sont corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$.

La convention consiste à réserver le symbole $\sqrt[3]{2}$ à la seule racine cubique réelle, c'est-à-dire α . Le corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$ sera engendré par $\sqrt[3]{2}$ et $j\sqrt[3]{2}$ (car il contient alors $j^2\sqrt[3]{2}$ qui est l'opposé de la somme de ces deux), mais aussi engendré par $\sqrt[3]{2}$ et j , ou encore par $\sqrt[3]{2}$ et $\sqrt{-3} = i\sqrt{3}$: c'est le corps $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$. On remarquera que la notation $\sqrt{-3}$ dans l'écriture $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ ne prête pas à confusion quant au résultat, d'après la remarque précédente.

• Ceci dit, si K est un corps arbitraire et x un élément de K , l'écriture « brute » $K(\sqrt[3]{x})$ n'a pas de sens en général, elle ne définit un corps qu'à un isomorphisme près, ce n'est pas un corps « concret », comme le montre l'exemple ci-dessus, si l'on n'a pas précisé quelle racine cubique de x on choisit dans le corps de rupture de $X^3 - x$ sur K . L'ambiguïté est levée si K contient les trois racines cubiques de l'unité, c'est-à-dire si $1 + X + X^2$ a ses racines dans K , ce qui signifie que -3 possède une racine carrée dans K . Alors peu importe le choix de la racine cubique pour $\sqrt[3]{x}$, le corps engendré contient les trois racines cubiques de x .

Les extensions successives.

On pourra bien sûr introduire des « extensions successives » de K , ce que l'on a d'ailleurs déjà vu dans le problème de la résolution d'une équation. Que devient alors le degré ?

Plus précisément, si l'on a des corps emboîtés $K \subset L \subset M$, que dire du degré $M : K$ du plus grand sur le plus petit par rapport aux degrés $M : L$ et $L : K$?

La réponse est simple. On va même prendre un cadre plus général, en prenant pour M un espace vectoriel sur L (qui n'est donc pas nécessairement un corps extension de L , ce qui signifie que l'on ne tient pas compte de la multiplication éventuelle dans M).

Restriction du corps des scalaires.

Pour respecter les traditions, on appellera donc E un espace vectoriel sur L . Comme K est sous-corps de L , E possède aussi une structure de K -espace, que l'on dit déduite de celle de L -espace par restriction du corps des scalaires. Comment passer d'une base et de la dimension de E sur L aux objets correspondants de E sur K ?

Pour simplifier, on supposera (et c'est d'ailleurs le seul cas intéressant) :

- E est de dimension finie sur le « grand corps » L ;
- le « grand corps » L est extension de degré fini du « petit corps » K .

Comme exemple, on part d'un espace vectoriel complexe E de dimension finie n sur $\mathbb{C}$. Quelle est la dimension de E sur $\mathbb{R}$? On peut remplacer bien sûr E par $\mathbb{C}^n$. Dans ces conditions, de la base canonique du $\mathbb{C}$ -espace $\mathbb{C}^n$ on déduit facilement la base suivante du $\mathbb{R}$ -espace $\mathbb{C}^n$, formée des $2n$ vecteurs :

$$\begin{array}{cccc} (1, 0, \dots, 0), & (0, 1, 0, \dots, 0), & \dots, & (0, 0, \dots, 0, 1), \\ (i, 0, \dots, 0), & (0, i, 0, \dots, 0), & \dots, & (0, 0, \dots, 0, i). \end{array}$$

En effet, tout élément du $\mathbb{R}$ -espace $\mathbb{C}^n$ s'écrit de manière unique sous la forme

$$(x_1 + iy_1, x_2 + iy_2, \dots, x_n + iy_n)$$

où les x_j et les y_j sont réels.

On en déduit donc

$$\dim_{\mathbb{R}} E = 2 \dim_{\mathbb{C}} E.$$

Or 2 est justement le degré de $\mathbb{C}$ sur $\mathbb{R}$.

La formule analogue dans le cas général est facile à montrer. Soit $(b_1, \dots, b_n)$ une base de E sur L et soit $(u_1, \dots, u_p)$ une base de L sur K . On aura donc

$$\dim_L E = n \quad \text{et} \quad L : K = p.$$

Tout $x \in E$ s'écrit de manière unique

$$x = \sum_{i=1}^n \alpha_i b_i$$

avec $\alpha_i \in L$.

Chaque coefficient α_i se décompose alors de manière unique sur la base de L

sur K , et il reste

Cette écriture
et $j = 1, \dots, p$,
Reste à mont.

Ceci donne

Or l'indépendance
l'indépendance
Une démonstration
on écrit

d'où

On a prouvé

Notons d'ailleurs
sur K , alors E est
conventions évi-

A

Énonçons :

S

F

La multiplicativ.

Une conséquence
successives.

sur K , et il reste une décomposition

$$x = \sum_{\substack{i=1, \dots, n \\ j=1, \dots, p}} \lambda_{ij} u_j b_i \quad \text{avec} \quad \lambda_{ij} \in K.$$

Cette écriture montre que la famille des np vecteurs $u_j b_i \in E$, pour $i = 1, \dots, n$ et $j = 1, \dots, p$, est totale dans le K -espace E .

Reste à montrer que cette famille est libre sur K . Écrivons donc

$$\sum_{\substack{i=1, \dots, n \\ j=1, \dots, p}} \mu_{ij} u_j b_i = 0 \quad \text{avec} \quad \mu_{ij} \in K.$$

Ceci donne

$$\sum_{i=1}^n \left(\sum_{j=1}^p \mu_{ij} u_j \right) b_i = 0.$$

Or l'indépendance des b_i sur L donne la nullité de $\sum_{j=1}^p \mu_{ij} u_j$ pour tout i , et l'indépendance des u_j sur K entraîne alors la nullité de tous les μ_{ij} .

Une démonstration plus concise utilise la distributivité des sommes directes : on écrit

$$L = \bigoplus_{j=1}^p K u_j \quad \text{et} \quad E = \bigoplus_{i=1}^n L b_i$$

d'où

$$E = \bigoplus_{i=1}^n \left(\bigoplus_{j=1}^p K u_j \right) b_i = \bigoplus_{\substack{i=1, \dots, n \\ j=1, \dots, p}} K u_j b_i.$$

On a prouvé la formule

$$\dim_L E = (L : K) \dim_K E.$$

Notons d'ailleurs que, si E est de dimension infinie sur L ou L de degré infini sur K , alors E est de dimension infinie sur K : la formule reste valable modulo les conventions évidentes.

Ainsi tout espace vectoriel sur $\mathbb{R}$ est de dimension infinie sur $\mathbb{Q}$.

Énonçons :

Si l'on restreint le corps des scalaires, la dimension est multipliée par le degré de l'extension.

La multiplicativité du degré.

Une conséquence essentielle est la « multiplicativité » des degrés d'extensions successives.

Soit $K \subset L \subset M$ une suite croissante de corps (on dit encore que L est un corps **intermédiaire** entre K et M). On peut écrire l'égalité

$$M : K = (M : L)(L : K)$$

le premier membre étant infini si l'un des deux facteurs du second l'est.

Le degré d'une extension d'extension est le produit des degrés.

Quelques conséquences :

- le degré de tout corps intermédiaire divise le degré de l'extension ;
- si le degré d'une extension de K est puissance d'un nombre premier, il en est de même du degré sur K de tout corps intermédiaire ;
- si M est de degré fini sur K , on peut écrire les équivalences

$$\begin{aligned} L = K &\Leftrightarrow M : K = M : L ; \\ L = M &\Leftrightarrow M : K = L : K ; \end{aligned}$$

- si L est de degré premier sur K , il n'y a pas, entre K et L , d'autres corps intermédiaires.

Une application aux corps finis.

Les propriétés de degré donnent beaucoup de renseignements dans le cas des corps finis.

En effet, si K est un corps fini, son sous-corps premier ne peut être le corps infini $\mathbb{Q}$, c'est donc un corps $\mathbb{Z}/p$ où p est un nombre premier, la caractéristique de K .

Mais K possède, sur son sous-corps $\mathbb{Z}/p$, un degré, nécessairement fini. Si n est ce degré, le $\mathbb{Z}/p$ -espace K est isomorphe au $\mathbb{Z}/p$ -espace $(\mathbb{Z}/p)^n$, comme tout espace de dimension finie. Le cardinal de K est donc celui de $(\mathbb{Z}/p)^n$, soit p^n .

Le cardinal d'un corps fini est une puissance de sa caractéristique, l'exposant étant le degré sur le sous-corps premier.

Une conséquence :

Si m possède deux facteurs premiers, il n'y a pas de corps de cardinal m .

Par contre, si m possède un seul facteur premier, soit p , il en est une puissance (on dit alors que m est un nombre primaire). On montre — et nous l'admettrons — que, pour tout entier primaire $m = p^n$, il existe un unique corps de cardinal p^n : c'est le corps de rupture de $X^{p^n} - X$ sur $\mathbb{Z}/p$, on le note

$$CG(p^n)$$

et on l'appelle **corps de Galois** de cardinal p^n (voir *Le Défi algébrique*, tome II, page 338).

Ainsi, $CG(p)$ n'est autre que le corps $\mathbb{Z}/p$.

Pour q
« grosseu
En effe

Les deg
respective

Autrem
t divise s
trons — c

Exercices.

1. L'en
degr
2. Calc
de 2.
3. Que
ratio
4. Calc.
5. Mon
muni
6. Mon
dédi.

Carac

7. Une

8. On c
donn

Mon
il en c
parm

Pour que $CG(p^s)$ soit extension de $CG(p^t)$, il est nécessaire, pour des raisons de « grosseur », que s soit supérieur à t . Mais ce n'est pas suffisant.

En effet, écrivons la multiplicativité des degrés dans la suite de corps

$$\mathbb{Z}/p = CG(p) \subset CG(p^t) \subset CG(p^s).$$

Les degrés de $CG(p^s)$ et de $CG(p^t)$ sur leur sous-corps premier $CG(p)$ étant respectivement s et t , il reste

$$s = (CG(p^s) : CG(p^t)) \cdot t.$$

Autrement dit, pour que $CG(p^s)$ soit extension de $CG(p^t)$, il est nécessaire que t divise s (pas seulement qu'il lui soit inférieur). On montre — et nous l'admettrons — que c'est suffisant, le degré de l'extension étant alors $\frac{s}{t}$.

Ainsi, $CG(p^3)$ n'est pas extension de $CG(p^2)$, il n'a aucun sous-corps de cardinal p^2 .

Par contre, $CG(p^4)$ possède un sous-corps de cardinal p^2 , sur lequel il est de degré 2.

Exercices.

1. L'ensemble des $a + b\sqrt{2}$, avec a et b dans $\mathbb{Q}$, est une extension de $\mathbb{Q}$. Quel est son degré ?
2. Calculer le degré sur $\mathbb{Q}$ du sous-corps de $\mathbb{C}$ engendré par la racine cubique réelle de 2. Que se passe-t-il si l'on prend une racine cubique non réelle ?
3. Que peut-on dire du degré sur $\mathbb{Q}$ du sous-corps de $\mathbb{C}$ engendré par un radical d'un rationnel ? Donner des exemples.
4. Calculer le degré sur $\mathbb{Q}$ du sous-corps de $\mathbb{C}$ engendré par $\sqrt{2} + \sqrt{3}$.
5. Montrer directement l'existence et l'unicité de corps de cardinal 4, 8, 9, en munissant d'une multiplication adéquate les groupes additifs $(\mathbb{Z}/2)^2$, $(\mathbb{Z}/2)^3$, $(\mathbb{Z}/3)^2$.
6. Montrer que $(1, X)$ est une base de $\mathbb{Q}(X)$ sur $\mathbb{Q}(X^2)$ et aussi sur $\mathbb{Q}(X^2 + X)$. En déduire les égalités

$$\mathbb{Q}(X) : \mathbb{Q}(X^2) = \mathbb{Q}(X) : \mathbb{Q}(X^2 + X) = 2.$$

Caractériser l'intersection K de $\mathbb{Q}(X^2)$ et $\mathbb{Q}(X^2 + X)$.

7. Une extension de degré 2 de K est engendrée sur K par tout élément hors de K .
8. On considère l'ensemble des extensions de K contenues dans une extension donnée L .

Montrer que c'est un treillis, c'est-à-dire que, pour deux telles extensions K_1 et K_2 , il en existe une maximale parmi celles contenues dans K_1 et K_2 , et une minimale parmi celles contenant K_1 et K_2 . On vérifiera que ce sont respectivement

l'intersection $K_1 \cap K_2$ et le produit (ou composé) $K_1 K_2$, sous-corps de L engendré par $K_1 \cup K_2$.

On suppose maintenant L de degré fini sur K . Le degré de $K_1 K_2$ sur K est alors un multiple commun des degrés de K_1 et K_2 sur K , et il est inférieur au produit de ces degrés.

Si l'un des degrés vaut 2, vérifier l'équivalence

$$(K_1 K_2 : K) = (K_1 : K)(K_2 : K) \Leftrightarrow K_1 \cap K_2 = K.$$

Est-elle vraie dans tous les cas ?

Étudier le cas où K_1 et K_2 sont les extensions de $\mathbb{Q}$ engendrées que $\sqrt{2}$ et i , par $\sqrt{2}$ et $\sqrt[3]{2}$, par $\sqrt[3]{2}$ et $j\sqrt[3]{2}$.

Reprenez
 $K(\alpha)$ engendré
Revoquez
puissances
l'ensemble
l'application

Cet ensemble
logique de
si, et seulement
nul y est in

D'où l'intersection
du noyau
d'anneaux

Les éléments

Un premier
l'une des pr

- l'élément
- la suite
- l'élément

On dit alors
infini puisqu

Si α est tr
valeur en α d

CORPS

engendré

t alors un
uit de ces

2 et i, par

Éléments algébriques sur un corps

Reprenons un élément α d'une extension d'un corps K . On a décrit le corps $K(\alpha)$ engendré par α sur K .

Revoyons-le pas à pas. Il contient K et α , donc la suite $(1, \alpha, \alpha^2, \dots)$ des puissances de α , donc les combinaisons K -linéaires de ces puissances, c'est-à-dire l'ensemble des valeurs en α des polynômes sur K , ou image de $K[X]$ par l'application « évaluation en α » :

$$P \rightarrow P(\alpha).$$

Cet ensemble des valeurs en α des polynômes sur K est un *anneau*, qu'il est logique de noter $K[\alpha]$. Ce sera un *corps* (donc le corps $K(\alpha)$ engendré par K et α) si, et seulement si, il est fermé par inversion, ce qui signifie que tout élément *non nul* y est inversible.

D'où l'intérêt de l'étude des polynômes $P \in K[X]$ s'annulant en α , c'est-à-dire du noyau de l'application ci-dessus (qui est un homomorphisme surjectif d'anneaux de $K[X]$ sur $K[\alpha]$).

Les éléments transcendants.

Un premier cas est celui où l'évaluation en α est injective, ce qui se traduit par l'une des propriétés suivantes :

- l'élément α n'est racine d'aucun polynôme non nul sur K ;
- la suite $(\alpha^n)_{n \in \mathbb{N}}$ des puissances de α est linéairement indépendante sur K ;
- l'élément α est algébriquement indépendant sur K (voir p. 25).

On dit alors que α est **transcendant** sur K . Le degré $K(\alpha) : K$ de $K(\alpha)$ sur K est infini puisque $K(\alpha)$ contient une famille infinie linéairement indépendante.

Le cas « étudié pour » est celui de l'indéterminée X , élément de $K(X)$ transcendant sur K .

Dans des cas concrets, la transcendance d'un élément donné n'est pas facile à prouver ! On a mis longtemps à montrer que π et e étaient des réels transcendants sur $\mathbb{Q}$, c'est-à-dire qu'ils n'annulent aucun polynôme non nul à coefficients rationnels (ou entiers, ça revient au même).

Si α est transcendant sur K , tout élément de l'anneau $K[\alpha]$ s'écrit comme valeur en α d'un *unique* polynôme sur K : dès lors, si $P(\alpha)$ est non nul, une égalité

$\frac{1}{P(\alpha)} = Q(\alpha)$ exige l'égalité $P(\alpha)Q(\alpha) = 1$, ce qui entraîne l'égalité $PQ = 1$ dans $K[X]$, donc P doit être une constante et $P(\alpha)$ doit être dans K .

En d'autres termes, seuls les éléments de $K \setminus 0$ sont inversibles dans $K[\alpha]$ (en particulier α ne l'est pas), ce dernier anneau n'est pas un corps, on doit adjoindre les inverses, et finalement les valeurs en α de toutes les fonctions rationnelles sur K (ces valeurs existent toujours grâce à la transcendance de α).

L'application

$$\begin{aligned} \frac{P}{Q} &\rightarrow P(\alpha)(Q(\alpha))^{-1} \\ K(X) &\rightarrow K(\alpha) \end{aligned}$$

est un homomorphisme injectif de corps, son image est un corps contenant K et α , c'est $K(\alpha)$ lui-même, et l'application est un isomorphisme.

Si α est transcendant sur K , l'extension $K(\alpha)$ s'identifie au corps des fractions rationnelles sur K .

Un élément transcendant « se comporte » donc comme une indéterminée. Notons en passant que la famille libre $(1, \alpha, \alpha^2, \dots)$ n'est pas une base du K -espace $K(\alpha)$, car elle n'est pas totale, elle n'engendre linéairement que le K -espace $K[\alpha]$. D'ailleurs on ne connaît pas explicitement de base de $K(\alpha)$ sur K .

Les éléments algébriques.

La non existence de polynômes $P \in K[X]$ non nuls ayant α pour racine réduit donc α au rôle d'une indéterminée sur K .

Plus intéressant est le cas contraire.

Une racine d'un polynôme non nul sur K est appelée un élément algébrique sur K .

C'est d'ailleurs un élément formant une famille algébriquement dépendante sur K (voir p. 25). Il est clair que les éléments algébriques forment une partie de la clôture algébrique de K ; on précisera plus tard s'il y a égalité.

- Tout élément de K est algébrique sur K : l'élément $\alpha \in K$ est en effet racine de

$$X - \alpha \in K[X] \setminus 0.$$

- Tout radical relatif à K est algébrique sur K : si β possède sa puissance n -ième dans K , il est racine de $X^n - \beta^n \in K[X] \setminus 0$.

- Les complexes $\sqrt{2}, i, j = \frac{-1 + i\sqrt{3}}{2}$ sont algébriques sur $\mathbb{Q}$, car ils ont une puissance dans $\mathbb{Q}$.

Il est cl
de K , ma

Premières

L'existe
l'existence

des puiss

En prat
qui soit c
suivantes

Plus pr
multiplier
(1, α , ...,
longueur
(lequel K)

• Un él
linéaireme

• Un é
engendré

En part
l'espace K
sur K .

- L'élément $\alpha = \sqrt{2} + \sqrt{3}$ n'est pas un radical relatif à $\mathbb{Q}$, aucune de ses puissances n'étant rationnelle. Néanmoins, il est algébrique sur $\mathbb{Q}$, comme le montre le calcul :

$$\begin{aligned}(\alpha - \sqrt{2})^2 &= 3 \\ \alpha^2 + 2 - 2\alpha\sqrt{2} &= 3 \\ \alpha^2 - 1 &= 2\alpha\sqrt{2} \\ (\alpha^2 - 1)^2 &= 8\alpha^2.\end{aligned}$$

On trouve α racine de

$$(X^2 - 1)^2 - 8X^2 = X^4 - 10X^2 + 1 \in \mathbb{Q}[X] \setminus 0.$$

- Tout complexe $z = a + ib$ est algébrique sur $\mathbb{R}$: il est racine de

$$X^2 - 2aX + a^2 + b^2 \in \mathbb{R}[X] \setminus 0.$$

Il est clair que, si un élément est algébrique sur K , il le reste sur toute extension de K , mais il peut ne plus l'être sur un sous-corps de K .

Un exemple *ad hoc* : π est dans $\mathbb{R}$, donc algébrique sur $\mathbb{R}$, donc aussi algébrique sur l'extension $\mathbb{C}$, mais il est transcendant sur le sous-corps $\mathbb{Q}$.

Premières caractérisations des éléments algébriques.

L'existence d'un polynôme non nul $P \in K[X]$ vérifiant $P(\alpha) = 0$ signifie l'existence d'une relation de dépendance dans la famille

$$(1, \alpha, \alpha^2, \dots)$$

des puissances de α .

En pratique, on peut écrire la suite des puissances de α jusqu'à en trouver une qui soit combinaison K -linéaire des précédentes; il est facile de voir que les suivantes sont encore combinaisons de celles-ci.

Plus précisément, si α^n est combinaison linéaire de $(1, \alpha, \dots, \alpha^{n-1})$, alors en multipliant par α on trouve α^{n+1} combinaison de $(\alpha, \alpha^2, \dots, \alpha^n)$, donc aussi de $(1, \alpha, \dots, \alpha^{n-1})$; de même pour $\alpha^{n+2}, \dots$. Il en résulte que cette suite finie de longueur n engendre le K -espace $K[\alpha]$ des valeurs en α des polynômes sur K (lequel $K[\alpha]$ est aussi l'anneau engendré par K et α).

- Un élément algébrique sur K est un élément dont la suite des puissances est linéairement dépendante sur K .

- Un élément algébrique sur K est un élément tel que le K -espace $K[\alpha]$ engendré par la suite de ses puissances soit de dimension finie.

En particulier, si l'on choisit un élément β dans une extension L de degré fini, l'espace $K[\beta]$ est sous-espace de L , donc de dimension finie, et β est algébrique sur K .

Tout élément d'une extension de degré fini est algébrique sur le corps.

La réciproque se déduira du paragraphe suivant, qui va prouver le résultat essentiel : si β est algébrique sur K , alors l'anneau $K[\beta]$ est un corps. Dans ces conditions $K(\beta)$ sera égal à $K[\beta]$, et β appartiendra bien à une extension de degré fini.

On pourra ainsi conclure à l'équivalence

$$\alpha \text{ algébrique sur } K \Leftrightarrow K(\alpha) : K < \infty.$$

Le corps engendré par un élément algébrique

Prenons l'élément $\alpha = \sqrt{2}$, algébrique sur $\mathbb{Q}$. Il est racine de $X^2 - 2 \in \mathbb{Q}[X]$

et la valeur en $\sqrt{2}$ de tout polynôme

$$P = a_0 + a_1X + \dots + a_nX^n \in \mathbb{Q}[X]$$

s'écrit sous la forme

$$P(\sqrt{2}) = (a_0 + 2a_2 + 4a_4 + \dots) + \sqrt{2}(a_1 + 2a_3 + 4a_5 + \dots).$$

En regroupant les termes pairs et impairs, on en déduit que les éléments de l'anneau $\mathbb{Q}[\sqrt{2}]$ s'écrivent tous sous la forme $u + v\sqrt{2}$, avec u et v dans $\mathbb{Q}$. D'ailleurs cette écriture est unique, 1 et $\sqrt{2}$ formant une base de $\mathbb{Q}[\sqrt{2}]$ sur $\mathbb{Q}$.

Pour avoir le corps $\mathbb{Q}(\sqrt{2})$ engendré par $\mathbb{Q}$ et $\sqrt{2}$, il faut adjoindre les inverses de ces éléments non nuls. Or le calcul

$$\frac{1}{u + v\sqrt{2}} = \frac{u}{u^2 - 2v^2} - \frac{v}{u^2 - 2v^2} \sqrt{2}$$

montre que l'inverse de tout élément non nul de $\mathbb{Q}[\sqrt{2}]$ est encore dans $\mathbb{Q}[\sqrt{2}]$.

Dès lors $\mathbb{Q}[\sqrt{2}]$ est un corps et il est égal à $\mathbb{Q}(\sqrt{2})$.

L'exemple ci-dessus n'est pas isolé : on va prouver que, si α est un élément algébrique sur K , alors $K[\alpha]$ est un corps, c'est-à-dire que l'inverse d'un polynôme en α (quand le polynôme ne s'annule pas en α) est encore un polynôme en α .

Pour cela, on va considérer, dans l'ensemble des polynômes non nuls sur K ayant α pour racine, ceux dont le degré est minimum ; parmi ceux-là, il y en a un seul de coefficient dominant égal à 1 (car sinon la différence de deux serait de degré strictement inférieur et s'annulerait en α). Appelons-le

$$M_\alpha = a_0 + a_1X + \dots + a_{n-1}X^{n-1} + X^n.$$

ÉLÉMENT

On va engendré

Dans ce strictement

s'écrit

et montre

Mais ce il existe T

On l'a mo Pour ce théorie des

• M_α es deux poly polynômes

• les se s'annule er reste doit

• si $Q(\alpha)$ M_α est irréc U et V vér

En subs $V(\alpha)Q(\alpha) = V \in K[X]$.

On a mont

algébrique sur le

ver le résultat
corps. Dans ces
condition de degré

est racine de

On va supposer α non nul (le cas $\alpha = 0$ offre peu d'intérêt, car alors le corps engendré est K).

Dans ces conditions a_0 est non nul, sinon $\frac{M_\alpha}{X}$ serait un polynôme de degré strictement inférieur à n s'annulant en α . Dès lors, l'égalité

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n = 0$$

s'écrit

$$\frac{1}{\alpha} = -a_0^{-1}(a_1 + a_2\alpha + \cdots + a_{n-1}\alpha^{n-2} + \alpha^{n-1})$$

et montre que l'inverse de α est encore un polynôme en α : donc $K[\alpha]$ contient $\frac{1}{\alpha}$.

Mais cela ne suffit pas : il faut montrer que, si $Q \in K[X]$ est non nul en α , il existe $T \in K[X]$ vérifiant

$$\frac{1}{Q(\alpha)} = T(\alpha).$$

On l'a montré ci-dessus pour $Q(X) = X$, mais il faut le cas général.

Pour cela, on montre successivement, en utilisant des résultats simples de théorie des anneaux :

- M_α est irréductible, c'est-à-dire qu'on ne peut pas l'écrire comme produit de deux polynômes non constants (caractère minimum du degré de M_α parmi les polynômes s'annulant en α);

- les seuls polynômes s'annulant en α sont les multiples de M_α (si $R \in K[X]$ s'annule en α , il en est de même du reste de sa division euclidienne par M_α , lequel reste doit donc être nul à cause du caractère minimum du degré de M_α);

- si $Q(\alpha)$ est non nul, alors Q n'est pas multiple de M_α dans $K[X]$ et, comme M_α est irréductible, Q et M_α sont premiers entre eux, donc il existe des polynômes U et V vérifiant l'identité de Bezout

$$UM_\alpha + VQ = 1.$$

En substituant l'indéterminée par α dans l'identité de Bezout, il reste $V(\alpha)Q(\alpha) = 1$, ce qui montre que l'inverse de $Q(\alpha)$ est la valeur en α du polynôme $V \in K[X]$.

En termes plus concis, le noyau de l'homomorphisme surjectif d'anneaux « évaluation en α »

$$\begin{array}{ccc} R & \rightarrow & R(\alpha) \\ K[X] & \rightarrow & K[\alpha] \end{array}$$

est l'idéal principal engendré par l'élément irréductible M_α , c'est donc un idéal maximal de $K[X]$ et le quotient est un corps. Or l'image $K[\alpha]$ est isomorphe au quotient de $K[X]$ par ce noyau, c'est donc aussi un corps.

On a montré :

Si α est algébrique sur K , le corps engendré par α sur K est l'ensemble des valeurs en α des polynômes sur K .

En comparant au cas où α est transcendant, on en déduit les nouvelles caractérisations suivantes du caractère algébrique de α :

- $K(\alpha) = K[\alpha]$;
- $K(\alpha) : K < \infty$;
- la suite des puissances de α engendre le K -espace $K[\alpha]$.

Une conséquence :

Les éléments algébriques sur un corps sont exactement les éléments de toutes les extensions de degré fini de ce corps.

Quelques exemples.

- L'exemple de $\sqrt{2}$ sur $\mathbb{Q}$ peut être généralisé à une extension $K(\alpha)$ où le carré de α est dans K .

Si l'on pose $\alpha^2 = u \in K$, un élément de $K[\alpha]$ s'écrit

$$P(\alpha) = a_0 + a_1\alpha + \dots + a_n\alpha^n \\ = (a_0 + a_2u + a_4u^2 + \dots) + \alpha(a_1 + a_3u + a_5u^2 + \dots).$$

On a regroupé les termes pairs et impairs, pour aboutir à

$$P(\alpha) = a + b\alpha$$

avec a et b dans K . Si $P(\alpha)$ est non nul, son inverse s'écrit

$$\frac{1}{a + b\alpha} = \frac{a}{a^2 - ub^2} - \frac{b}{a^2 - ub^2}\alpha.$$

Il est bien égal à un polynôme en α .

- Le nombre réel $x = \sqrt[3]{1 - \sqrt{2}}$ est algébrique sur $\mathbb{Q}$: il vérifie en effet $(x^3 - 1)^2 = 2$, donc il est racine du polynôme

$$X^6 - 2X^3 - 1.$$

L'élément $y = x^2 + 1$ est dans $K(x) \setminus \mathbb{Q}$ donc, d'après ce qui précède, son inverse doit s'écrire comme un polynôme en x .

Pour le trouver, recopions la méthode ci-dessus : le polynôme $X^2 + 1$ est premier avec

$$X^6 - 2X^3 - 1.$$

On doit alors chercher une identité de Bezout entre

$$P = X^6 - 2X^3 - 1 \quad \text{et} \quad Q = X^2 + 1.$$

Ceci se fait par divisions euclidiennes. On commence par diviser P par Q :

$$X^6 - 2X^3 - 1 = (X^2 + 1)(X^4 - X^2 - 2X + 1) + 2(X - 1)$$

puis on divise Q par le reste $X - 1$:

$$X^2 + 1 = (X - 1)(X + 1) + 2.$$

On multiplie alors la première égalité de division par $X + 1$, ce qui donne

$$(X^6 - 2X^3 - 1)(X + 1) = (X^2 + 1)(X + 1)(X^4 - X^2 - 2X + 1) + 2(X^2 + 1) - 4.$$

C'est là une identité de Bezout cherchée. Et si l'on y substitue X par $x = \sqrt[3]{1 - \sqrt{2}}$, il reste

$$0 = (x^2 + 1)(x + 1)(x^4 - x^2 - 2x + 1) + 2(x^2 + 1) - 4$$

ou encore

$$\frac{4}{x^2 + 1} = (x + 1)(x^4 - x^2 - 2x + 1) + 2.$$

L'inverse de $y = x^2 + 1$ est donc

$$\frac{1}{y} = \frac{1}{4}(x^5 + x^4 - x^3 - 3x^2 - x + 3);$$

il est bien égal à un polynôme en x .

• Soit α un élément algébrique racine de $X^8 - 3X + 5$. Considérons $\beta = 1 - \alpha$. Une division euclidienne donne

$$X^8 - 3X + 5 = (1 - X)Q + 3$$

(en substituant X par 1), d'où l'égalité

$$0 = (1 - \alpha)Q(\alpha) + 3$$

qui montre que $\beta = 1 - \alpha$ est non nul, son inverse étant

$$\frac{1}{\beta} = -\frac{Q(\alpha)}{3}.$$

Reste à calculer

$$Q = \frac{X^8 - 3X + 2}{1 - X} = -(X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X - 2)$$

d'où la valeur

$$\frac{1}{1 - \alpha} = \frac{1}{3}(\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha - 2).$$

• Pour le même nombre complexe α , prenons

$$\gamma = \alpha^{10} + \alpha^5 - 3\alpha^3 + 5\alpha^2 - \alpha.$$

On réduit d'abord le degré en divisant par $X^8 - 3X + 5$, qui

possède α pour racine :

$$X^{10} + X^5 - 3X^3 + 5X^2 - X = (X^8 - 3X + 5)X^2 + X^5 - X.$$

Cette égalité montre que γ est aussi égal à $\alpha^5 - \alpha$. Pour calculer son inverse (s'il est non nul), on procède encore par divisions euclidiennes :

$$X^8 - 3X + 5 = (X^5 - X)X^3 + X^4 - 3X + 5$$

d'où

$$0 = (\alpha^5 - \alpha)\alpha^3 + \alpha^4 - 3\alpha + 5.$$

On recommence :

$$X^5 - X = (X^4 - 3X + 5)X + 3(X^2 - 2X).$$

On multiplie alors la précédente égalité par α et on remplace $\alpha(\alpha^4 - 3\alpha + 5)$ par $(\alpha^5 - \alpha) - 3(\alpha^2 - 2\alpha)$. Il reste

$$0 = (\alpha^5 - \alpha)(\alpha^4 + 1) - 3(\alpha^2 - 2\alpha).$$

Nouvelle division

$$X^5 - X = (X^2 - 2X)(X^3 + 2X^2 + 4X + 8) + 15X$$

suivie par la multiplication de l'égalité antérieure par

$$\alpha^3 + 2\alpha^2 + 4\alpha + 8.$$

On tombe sur

$$0 = (\alpha^5 - \alpha)[(\alpha^4 + 1)(\alpha^3 + 2\alpha^2 + 4\alpha + 8) - 3] + 45\alpha.$$

$$0 = (\alpha^5 - \alpha)(\alpha^7 + 2\alpha^6 + 4\alpha^5 + 8\alpha^4 + \alpha^3 + 2\alpha^2 + 4\alpha + 5) + 45\alpha.$$

Avant de diviser par α , on remplace, dans la parenthèse, 5 par $3\alpha - \alpha^8$, qui lui est égal. Il reste après division par α (qui est non nul)

$$0 = (\alpha^5 - \alpha)(-\alpha^7 + \alpha^6 + 2\alpha^5 + 4\alpha^4 + 8\alpha^3 + \alpha^2 + 2\alpha + 7) + 45.$$

Cette égalité montre que $\alpha^5 - \alpha = \gamma$ n'est pas nul, et donne son inverse

$$\frac{1}{\alpha^5 - \alpha} = \frac{1}{45}(\alpha^7 - \alpha^6 - 2\alpha^5 - 4\alpha^4 - 8\alpha^3 - \alpha^2 - 2\alpha - 7).$$

Les extensions algébriques d'un corps.

Il est naturel d'appeler **extension algébrique** d'un corps une extension dont tout élément est algébrique sur ce corps. Une extension possédant au moins un élément transcendant s'appellera alors une **extension transcendante** du corps de base.

- Toute extension de degré fini est algébrique : on l'a déjà vu précédemment.

Exercices.

1. Dans polyn

(dans
ration

$+X^5 - X$.

z. Pour calculer
e par divisions

$X + 5$

$2X$).

et on remplace
este

).

$8) + 15X$

e par

$5) + 45x$.

renthèse, 5 par
t α (qui est non

$2x + 7) + 45$.

l, et donne son

$-2x - 7$).

nsion dont tout
au moins un
te du corps de

on l'a déjà vu

• On montrera que la clôture algébrique est une extension algébrique (voir p. 98).

• Une extension peut être de degré infini tout en étant algébrique : c'est le cas de la saturation par radicaux de $\mathbb{Q}$ ou de la clôture algébrique de $\mathbb{Q}$. En effet, ces extensions ont des éléments de degré aussi grand qu'on veut, car il y a sur $\mathbb{Q}$ des polynômes irréductibles de degré aussi grand qu'on veut (exemple de $1 + X + \dots + X^{p-1}$ pour p premier).

• Un corps algébriquement clos n'a pas d'extension algébrique propre, d'où il résulte que la clôture algébrique d'un corps est une extension algébrique maximale.

• Si $z = a + ib$ est un complexe non réel, l'extension $\mathbb{R}(z)$ contient $i = b^{-1}(z - a)$. D'ailleurs, elle est de degré strictement supérieur à 1 et est contenue dans $\mathbb{C}$ qui est de degré 2. On en déduit $\mathbb{R}(z) = \mathbb{C}$, d'où :

les seules extensions algébriques de $\mathbb{R}$ sont $\mathbb{R}$ et $\mathbb{C}$.

• Si $\alpha_1, \dots, \alpha_n$ sont algébriques sur K , l'extension $K(\alpha_1, \dots, \alpha_n)$ est une extension algébrique de K , formée de l'ensemble des valeurs en $(\alpha_1, \dots, \alpha_n)$ de tous les polynômes à n indéterminées sur K : si $P \in K[X_1, \dots, X_n]$ ne s'annule pas en $(\alpha_1, \dots, \alpha_n)$, alors

$$\frac{1}{P(\alpha_1, \dots, \alpha_n)} \quad \text{s'écrit} \quad Q(\alpha_1, \dots, \alpha_n)$$

pour un certain $Q \in K[X_1, \dots, X_n]$ (le vérifier).

On peut d'ailleurs remplacer les α_i par une partie quelconque, finie ou infinie, d'éléments algébriques sur K : l'extension est toujours algébrique.

Exercices.

1. Dans les exemples suivants, montrer que α est algébrique sur $\mathbb{Q}$, et calculer, comme polynôme en x , l'inverse de $\alpha + 1$ et l'inverse de $\alpha^3 + 1$:

$$\alpha = \sqrt{2} + \sqrt{3}$$

$$\alpha = 1 + \sqrt[4]{2}$$

$$\alpha = \frac{1}{1 - \sqrt{2}}$$

$$\alpha \text{ racine de } X^3 - X - 1$$

$$\alpha \text{ racine de } X^2 + iX + 2$$

(dans ce dernier cas, on commencera par chercher un polynôme à coefficients rationnels dont α est racine).

2. Si α est transcendant sur K , montrer qu'il est algébrique sur $K(\alpha^2)$ et sur $K\left(\frac{1}{\alpha^3}\right)$:
on pourra considérer respectivement les polynômes

$$X^2 - \alpha^2 \quad \text{et} \quad X^3 \left(\frac{1}{\alpha^3}\right) - 1.$$

Plus généralement, si P et Q sont dans $K[X] \setminus 0$, α est racine de

$$Q(X) \frac{P(\alpha)}{Q(\alpha)} - P(X)$$

polynôme à coefficients dans $K\left(\frac{P(\alpha)}{Q(\alpha)}\right)$. En déduire qu'un élément α transcendant sur K est algébrique sur tout corps intermédiaire entre K et $K(\alpha)$ et contenant strictement K .

3. Si L est une extension de degré fini de K , tout anneau entre K et L est un corps.
4. Si L est extension algébrique de H et H extension algébrique de K , alors L est extension algébrique de K (c'est ce que l'on appelle la transistivité de l'algébraïcité).
On pourra commencer par le cas où H est de degré fini sur K , puis prendre $x \in L$ et ramener le problème de l'algébraïcité de x sur K au cas précédent, en considérant les coefficients d'un polynôme sur H dont x est racine.
5. Soit L une extension de K de degré fini. On prend un élément x algébrique sur K (tout cela dans un « grand corps » contenant L et x). Une base de L sur K est-elle aussi base de $L(x)$ sur $K(x)$?
6. L'existence de nombres réels transcendants sur $\mathbb{Q}$ se déduit du fait que l'ensemble des réels algébriques sur $\mathbb{Q}$ est dénombrable (alors que $\mathbb{R}$ ne l'est pas). Plus précisément, on prouvera successivement :
- si, pour tout $P \in \mathbb{Z}[X]$, on appelle $h(P)$ la somme du degré de P et des modules de ses coefficients, alors pour tout entier m il n'y a qu'un nombre fini de P vérifiant

$$h(P) \leq m;$$

- l'ensemble $\mathbb{Z}[X]$ est dénombrable;
- l'ensemble des nombres algébriques sur $\mathbb{Q}$ est dénombrable.

7. La démonstration ci-dessus n'est pas constructive, elle n'« exhibe » aucun réel transcendant sur $\mathbb{Q}$.

Un des premiers que l'on ait trouvé est la somme de la série de terme général $\frac{1}{10^{(n!)}}$

soit $\alpha = \sum_{n \geq 1} 10^{-(n!)}$. Pour le prouver, on va démontrer une certaine propriété que

vérifie tout nombre algébrique et que ne vérifie pas α .

Partons de x algébrique sur $\mathbb{Q}$, racine d'un polynôme T de degré $m \geq 1$ à coefficients entiers.

On vérifiera successivement :

- si $\frac{p}{q} \in \mathbb{Q}$ n'est pas racine de T , alors $\left|T\left(\frac{p}{q}\right)\right|$ est supérieur à $\frac{1}{q^m}$;
- si x n'est pas rationnel et s'il est la racine de T la plus proche d'un rationnel

$\frac{p}{q} \in]x$
major
des ac
• pou
coupl

On en

et sur $K\left(\frac{1}{\alpha^3}\right)$:

$\frac{p}{q} \in]x - 1, x + 1[$, alors la distance de x à $\frac{p}{q}$ est supérieure à $M^{-1}q^{-m}$, M étant un majorant du module de la dérivée T' dans $]x - 1, x + 1[$ (on utilisera le théorème des accroissements finis);

• pour tout entier t supérieur à $(m + 1)$ et tout entier $k > 0$, seul un nombre fini de couples (p, q) d'entiers premiers entre eux vérifie l'inégalité

$$\left|x - \frac{p}{q}\right| < kq^{-t}.$$

On en déduira que α n'est pas algébrique sur $\mathbb{Q}$.

transcendant

) et contenant

est un corps.

K , alors L est
l'algèbre (ité).

rendre $x \in L$ et
en considérant

algébrique sur K
sur K est-elle

que l'ensemble
est pas). Plus

des modules de
de P vérifiant

« aucun réel

général $\frac{1}{10^{(n)}}$

propriété que

degré $m \geq 1$ à

d'un rationnel

Le polynôme minimum d'un élément algébrique

Pour un élément algébrique x sur K , on a signalé, parmi les polynômes à coefficients dans K dont il est racine, l'existence et l'unicité d'un de degré minimum et à coefficient dominant égal à 1.

On l'appelle le **polynôme minimum** de x sur K et on le note M_x . En fait, on n'exige souvent pas la condition sur le coefficient dominant, ce qui revient à définir M_x à un facteur constant non nul près. C'est alors le seul polynôme irréductible sur K s'annulant en x , si bien que dès que l'on « tombe » sur un polynôme irréductible $P \in K[X]$ vérifiant $P(x) = 0$, on peut affirmer que P est le polynôme minimum de x sur K (et aussi celui de toutes ses autres racines éventuelles dans le corps de rupture).

On n'oubliera pas qu'aux degrés 2 et 3 l'irréductibilité équivaut à l'absence de racines dans le corps de base.

Le degré d'un élément algébrique.

Si x est algébrique sur K , le degré n de son polynôme minimum M_x est aussi le degré de l'extension $K(x)$ sur K ; on l'appelle **degré** de x sur K , et une base du K -espace $K(x)$ est alors $(1, x, x^2, \dots, x^{n-1})$. On étend la notion de degré à un élément transcendant, en le posant bien sûr égal à l'infini.

Le degré de x sur K est aussi la plus petite puissance qui dépend linéairement, sur K , des précédentes. Il divise le degré, sur K , de toute extension L de K qui contient x : ce résultat essentiel résulte de la multiplicativité des degrés dans la chaîne $K \subset K(x) \subset L$.

On sait que tout élément de $K(x)$ est la valeur en x d'un polynôme sur K . On peut ajouter que c'est la valeur en x d'un *unique* polynôme sur K de degré strictement inférieur à n : pour $P \in K[X]$, l'élément $P(x) \in K(x)$ est aussi égal à la valeur en x du reste de la division euclidienne de P par M_x .

On peut donc *identifier* $K(x)$ avec l'ensemble des polynômes de degré inférieur à $(n - 1)$, la somme étant la somme usuelle, mais le produit de P et Q étant égal au reste de la division euclidienne du produit PQ par M_x .

Des exemples.

- Le polynôme $X^2 - 2$ étant irréductible sur $\mathbb{Q}$, on retrouve le fait que tout élément de $\mathbb{Q}(\sqrt{2})$ s'écrit de manière unique $a + b\sqrt{2}$ avec a et b dans $\mathbb{Q}$.

• Si α est non nul algébrique sur K , il en est de même de son inverse. Les extensions $K(\alpha)$ et $K\left(\frac{1}{\alpha}\right)$ sont d'ailleurs identiques, et le polynôme minimum de $\frac{1}{\alpha}$ sur K est le polynôme réciproque de celui de α sur K : si M_α est celui de α , de degré n , celui de $\frac{1}{\alpha}$ est $X^n M_\alpha\left(\frac{1}{X}\right)$, à des facteurs constants près bien sûr.

• La racine cubique $j = \frac{-1 + i\sqrt{3}}{2}$ de 1 annule le polynôme $X^3 - 1$, mais ce dernier est réductible sur $\mathbb{Q}$, il s'écrit

$$(X - 1)(X^2 + X + 1).$$

Or j n'annule pas $X - 1$, dont il annule $X^2 + X + 1$, qui est irréductible sur $\mathbb{Q}$ (car son discriminant vaut -3 , et n'a pas de racine carrée dans $\mathbb{Q}$).

En conclusion : le polynôme minimum de j sur $\mathbb{Q}$ est $1 + X + X^2$, donc j est de degré 2 sur $\mathbb{Q}$.

On retrouve ce résultat en remarquant que $\mathbb{Q}(j)$ est identique à $\mathbb{Q}(i\sqrt{3})$, les éléments s'écrivant indifféremment $a + bj$ dans la base $(1, j)$ ou $c + di\sqrt{3}$ dans la base $(1, i\sqrt{3})$, (a, b, c, d rationnels).

• Plus généralement, une racine n -ième de l'unité autre que 1 est racine de $X^n - 1$, donc aussi de

$$\frac{X^n - 1}{X - 1} = 1 + X + X^2 + \cdots + X^{n-1}.$$

Le corps de base étant $\mathbb{Q}$, ce polynôme

$$T_n = 1 + X + X^2 + \cdots + X^{n-1}$$

n'est pas toujours irréductible.

Si T_n est irréductible sur $\mathbb{Q}$, alors les $(n - 1)$ racines n -ièmes de l'unité autres que 1 ont T_n pour polynôme minimum sur $\mathbb{Q}$. On montre que c'est le cas si n est premier (voir *Le défi algébrique*, tome II, page 336).

Ainsi, le polynôme minimum de $e^{\frac{2i\pi}{5}}$ est

$$1 + X + X^2 + X^3 + X^4,$$

c'est aussi celui de

$$e^{\frac{4i\pi}{5}}, \quad e^{\frac{6i\pi}{5}}, \quad e^{\frac{8i\pi}{5}}.$$

• Pour $n = 4$, le polynôme T_4 s'écrit

$$1 + X + X^2 + X^3 = (1 + X)(1 + X^2).$$

Heureusement : car -1 est racine quatrième de l'unité, et les deux autres sont i et $-i$, de polynôme minimum $X^2 + 1$.

- Les racines sixièmes de l'unité autres que 1 sont

$$-1, \quad j, \quad j^2, \quad -j, \quad -j^2,$$

les polynômes minima étant $1 + X$ pour la première, $1 + X + X^2$ pour les deux suivantes et $1 - X + X^2$ pour les deux dernières. On vérifie la factorisation de T_6 :

$$1 + X + X^2 + X^3 + X^4 + X^5 = (1 + X)(1 + X + X^2)(1 - X + X^2).$$

- Comme racines douzièmes de l'unité, il y a déjà 1 et -1 comme racines carrées, puis i et $-i$ comme racines quatrièmes, et j et j^2 comme racines cubiques. Le polynôme $X^{12} - 1$ doit donc être divisible, dans $\mathbb{Q}[X]$, par

$$(X^2 - 1)(X^2 + 1)(X^2 + X + 1) = X^6 + X^5 + X^4 - X^2 - X - 1.$$

On trouve comme quotient

$$\frac{X^{12} - 1}{X^6 + X^5 + X^4 - X^2 - X - 1} = X^6 - X^5 + X^3 - X + 1.$$

La racine $e^{\frac{2i\pi}{12}}$, n'ayant 1 ni pour carré, ni pour cube, ni pour puissance quatrième, annule ce polynôme. Mais il en est de même des racines douzièmes de l'unité qui ne sont pas racines carrées ni cubiques, c'est-à-dire $-j$ et $-j^2$, lesquelles ont $X^2 - X + 1$ pour polynôme minimum.

Donc $e^{\frac{2i\pi}{12}}$ annule le quotient

$$\frac{X^6 - X^5 + X^3 - X + 1}{X^2 - X + 1} = X^4 - X^2 + 1.$$

C'est d'ailleurs prévisible, car le carré de $e^{\frac{2i\pi}{12}}$ n'est autre que $e^{\frac{2i\pi}{6}} = -j^2$ qui est racine de

$$X^2 - X + 1.$$

On peut faire le calcul explicite :

$$e^{\frac{2i\pi}{12}} = \cos \frac{\pi}{6} + i \sin \frac{\pi}{6} = \frac{\sqrt{3} + i}{2}.$$

Comme $X^4 - X^2 + 1$ n'a pas de racine dans $\mathbb{Q}$ (car $X^2 - X + 1$ n'en a déjà pas), sa seule factorisation possible serait en produit de polynômes de degré 2, donc $e^{\frac{2i\pi}{12}}$ serait alors de degré 2 sur $\mathbb{Q}$ et sa somme avec son conjugué complexe serait dans $\mathbb{Q}$: c'est faux, car elle vaut $\sqrt{3}$.

Un retour sur

Si le carré d'une extension de degré 2, donc toute extension de degré 4, est une extension de degré 2, donc toute extension de degré 4 est une extension de degré 2.

Partant d'une extension de degré 2, on déduit que les racines d'un polynôme de degré 4 sont forcément de la même manière concues.

C'est une conséquence pour le degré sur les corps à par

de l'unité, et les
um $X^2 + 1$.

sont

j^2 ,

ière, $1 + X + X^2$
s deux dernières.

$^2)(1 - X + X^2)$.

à 1 et -1 comme
atrièmes, et j et j^2
1 doit donc être

$-X^2 - X - 1$.

$+ X^3 - X + 1$.

ur cube, ni pour
il en est de même
racines carrées ni
ont $X^2 - X + 1$

$^2 + 1$.

n'est autre que

i .

car $X^2 - X + 1$
serait en produit
e degré 2 sur $\mathbb{Q}$ et
ns $\mathbb{Q}$: c'est faux,

Conclusion : $X^4 - X^2 + 1$ est irréductible sur $\mathbb{Q}$, et
 $e^{\frac{2i\pi}{12}} = \frac{\sqrt{3} + i}{2}$ est de degré 4 sur $\mathbb{Q}$.

• Le degré d'un radical relatif à K est facilement majoré : si x est une racine n -ième d'un élément α de K , x est racine de $X^n - \alpha$, son degré est inférieur à n , et il sera égal à n si, et seulement si, $X^n - \alpha$ est irréductible sur K .

• On a trouvé que l'élément $x = \sqrt[3]{1 - \sqrt{2}}$ était racine du polynôme rationnel

$$(X^3 - 1)^2 - 2 = X^6 - 2X^3 - 1.$$

Ce sera là son polynôme minimum si, et seulement si, il est irréductible sur $\mathbb{Q}$. Commençons par le décomposer sur $\mathbb{R}$:

$$\begin{aligned} X^6 - 2X^3 - 1 &= (X^3 - 1 + \sqrt{2})(X^3 - 1 - \sqrt{2}) \\ &= (X - x)(X^2 + xX + x^2)(X - y)(X^2 + yX + y^2) \end{aligned}$$

On a posé $y = \sqrt[3]{1 + \sqrt{2}}$ (les radicaux sont tous réels) et, les polynômes de degré 2 n'ayant pas de racine réelle, on est en présence de la décomposition en facteurs premiers dans $\mathbb{R}[X]$.

Il est facile de vérifier qu'aucun groupement de ces facteurs premiers réels ne donne un polynôme rationnel : le polynôme est donc irréductible sur $\mathbb{Q}$ et x est de degré 6 sur $\mathbb{Q}$.

Un retour sur les nombres constructibles.

Si le carré de α est dans K , le degré de α sur K est 1 ou 2 ; par multiplicativité, toute extension de K par racines carrées successives a pour degré une puissance de 2, donc tous ses éléments ont aussi pour degré sur K une puissance de 2.

Partant d'une partie P du plan, symétrique par rapport à l'axe réel, on en déduit que les nombres constructibles à la règle et au compas à partir de P sont forcément de degré puissance de 2 sur $\mathbb{Q}(P)$, corps engendré par P . On dira de manière concise :

Un nombre constructible à la règle et au compas a pour degré une puissance de 2.

C'est une condition *nécessaire*, un résultat « négatif » : ainsi, si $z \in \mathbb{C}$ n'a pas pour degré sur $\mathbb{Q}$ une puissance de 2, il n'est pas constructible à la règle et au compas à partir de 0 et 1.

• Le degré de $\sqrt[3]{2}$ sur $\mathbb{Q}$ est 3, car le polynôme $X^3 - 2$ est irréductible sur $\mathbb{Q}$.

Conclusion : réponse négative à la duplication du cube.

- La trisection d'un angle de 60° correspond au problème de la constructibilité de $\alpha = \cos 20^\circ + i \sin 20^\circ$ à partir de 0, 1, et

$$\cos 60^\circ + i \sin 60^\circ = -j^2.$$

Le corps engendré par ces éléments est $\mathbb{Q}(j)$, et $\alpha = e^{\frac{2i\pi}{3}}$ vérifie $\alpha^3 = -j^2$, donc est racine de

$$X^3 + j^2 \in \mathbb{Q}(j)[X].$$

Si l'on montre que $X^3 + j^2$ est irréductible sur $\mathbb{Q}(j)$, α sera de degré 3, donc non constructible.

Supposons donc $X^3 + j^2$ réductible sur $\mathbb{Q}(j)$. En prenant les conjugués complexes et en multipliant, on trouve que

$$(X^3 + j^2)(X^3 + j) = X^6 - X^3 + 1$$

est réductible sur $\mathbb{Q}$.

On va montrer que c'est faux, en prouvant (par le critère d'Eisenstein) l'irréductibilité de $A = X^6 - X^3 + 1$ sur $\mathbb{Q}$. Dans

$$A(X) = X^6 - X^3 + 1$$

on fait la substitution $X = -1 - Y$, et il suffit de prouver que

$$B(Y) = A(-1 - Y)$$

est irréductible. On calcule

$$B(Y) = (Y + 1)^6 + (Y + 1)^3 + 1.$$

Si l'on avait une factorisation propre $B = ST$ dans $\mathbb{Q}[Y]$, on l'aurait dans $\mathbb{Z}[Y]$, d'après un résultat facile (il suffit de l'écrire...). Passons dans $\mathbb{Z}/3[Y]$. On vérifie que tous les coefficients de B autres que le dominant sont multiples de 3, donc il reste $Y^6 = \bar{S}\bar{T}$ dans $\mathbb{Z}/3[Y]$. Par suite $\bar{S}$ et $\bar{T}$, n'étant pas constants (car S et T ne le sont pas et ils ont 1 pour coefficient dominant), sont des puissances de Y dans $\mathbb{Z}/3[Y]$, et leur terme constant est nul. Si l'on revient à $\mathbb{Z}[Y]$, les termes constants de S et T sont multiples de 3, celui de B doit donc être multiple de 9, ce qui est faux car il vaut 3.

On a bien montré que $e^{\frac{2i\pi}{3}}$ est de degré 3 sur $\mathbb{Q}(j)$. Conclusion : impossibilité de diviser en trois l'angle de 60° avec une règle et un compas.

La dépendance du degré sur le corps de base.

Si l'on « augmente » le corps de base, un élément algébrique reste algébrique, mais son degré peut diminuer.

Plus précisément, si x est algébrique sur K et si L est une extension de K , soit $K \subset L$, le polynôme minimum M_x de x sur K est aussi un polynôme sur L , donc

LE POLY

x est algébrique

- ou bien polynôme

- ou bien inférieur à M_x dans

Adjonction

Si x et y de y à $K(x)$, degré de y

D'ailleurs et seulement minimum

Bien entendu $x_1, \dots, x_q$ inférieur au

Réciproquement d'un nombre à un des éléments degrés augmenté

D'où l'équation

où les α_i sont

Somme et produit

Reprenons sur K , contenu dans K , et chaque produit

problème de la
de 0, 1, et

$= e^{\frac{2i\pi}{18}}$ vérifie

(j), α sera de

prenant les
que

ar le critère
sur $\mathbb{Q}$. Dans

prouver que

x est algébrique sur K . Dès lors :

- ou bien M_x reste irréductible sur L , et alors x a même degré et même polynôme minimum sur K et sur L ;
- ou bien M_x est réductible sur L , auquel cas le degré de x sur L est strictement inférieur à son degré sur K , son polynôme minimum sur L étant un diviseur strict de M_x dans $L[X]$.

Le cas « caricatural » consiste à prendre x hors de K , et pour L l'extension $K(x)$ elle-même. Le degré de x sur $K(x)$ est toujours 1, le polynôme minimum étant $X - x$.

Adjonction de plusieurs éléments algébriques.

Si x et y sont algébriques sur K , l'extension $K(x, y)$ s'obtient par adjonction de y à $K(x)$. Le degré $K(x, y) : K$ est égal au produit du degré de x sur K par le degré de y sur $K(x)$, lequel est *inférieur* au degré de y sur K .

D'ailleurs, le degré $K(x, y) : K$ sera égal au produit des degrés de x et y sur K si, et seulement si, y a même degré sur $K(x)$ et sur K , ce qui signifie que le polynôme minimum de y sur K est irréductible sur $K(x)$.

Ainsi, $X^2 + 1$ est irréductible sur tout sous-corps de $\mathbb{R}$, donc i est de degré 2 sur $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(i, \sqrt{2})$ est de degré 4 sur $\mathbb{Q}$. Une base est $(1, \sqrt{2}, i, i\sqrt{2})$, et tout élément s'écrit de manière unique

$$a + b\sqrt{2} + ci + di\sqrt{2}$$

avec a, b, c, d rationnels.

Bien entendu, on peut adjoindre à K un nombre fini d'éléments algébriques $x_1, \dots, x_q$: on obtiendra une extension algébrique $K(x_1, \dots, x_q)$, de degré fini inférieur au produit des degrés des x_i .

Réciproquement, toute extension de degré fini de K s'obtient par adjonction d'un nombre fini d'éléments algébriques : on procède pas à pas, en adjoignant un à un des éléments du complémentaire, et on doit s'arrêter à un moment car les degrés augmentent strictement.

D'où l'équivalence

$$L : K < \infty \Leftrightarrow L = K(\alpha_1, \dots, \alpha_n)$$

où les α_i sont algébriques sur K .

Somme et produit d'éléments algébriques.

Reprenons x et y algébriques sur K . L'extension $K(x, y)$, qui est de degré fini sur K , contient entre autres $(x + y)$ et xy , qui sont par conséquent algébriques sur K , et chacun de degré inférieur au degré de $K(x, y)$ sur K , *a fortiori* inférieur au produit des degrés de x et y sur K .

La somme et le produit de deux éléments algébriques sont aussi algébriques.

Le résultat ci-dessus ne dit rien sur les polynômes annulés par $(x + y)$ ou xy , en particulier sur leurs polynômes minima.

En fait, si p et q sont les degrés de x et y sur K , on va voir une méthode pour écrire un polynôme de degré pq ayant $(x + y)$ pour racine : mais ce ne sera pas forcément le polynôme minimum, car il peut être réductible.

Pour cela, on va écrire la suite des racines du polynôme minimum M_x de x sur K ; ces racines sont par exemple dans la clôture algébrique de K , l'une d'elles est x , et la suite $x = x_1, x_2, \dots, x_p$ est telle que toutes ses fonctions symétriques élémentaires, donc toutes ses fonctions symétriques, sont dans K (car elles s'expriment rationnellement à l'aide des coefficients de M_x). Les x_i , que l'on appelle **conjugués** de x sur K , apparaîtront souvent dans la suite.

De même pour y , on prend la suite $y = y_1, y_2, \dots, y_q$ des racines de M_y . La somme $(x + y)$ n'a aucune raison d'être dans K , on va lui associer les pq sommes $(x_i + y_j)$ de manière à « symétriser » et l'on va considérer le polynôme

$$M = \prod_{\substack{i=1, \dots, p \\ j=1, \dots, q}} (X - (x_i + y_j)).$$

Il est clair que $(x + y) = (x_1 + y_1)$ est racine de M et l'on va montrer que les coefficients de M sont dans K , ce qui prouvera d'ailleurs directement que $x + y$ est algébrique sur K et de degré inférieur à pq .

Or un coefficient arbitraire de M est la valeur en $(x_1, \dots, x_p, y_1, \dots, y_q)$ d'un certain polynôme

$$T(X_1, \dots, X_p, Y_1, \dots, Y_q)$$

à $(p + q)$ indéterminés sur K , invariant par toute permutation des X_i et toute permutation des Y_j .

Il est facile de voir qu'il s'exprime à l'aide des polynômes symétriques élémentaires des X_i et des Y_j . On le fait en deux étapes, en considérant d'abord T comme polynôme symétrique en $(Y_1, \dots, Y_q)$ à coefficients dans $K(X_1, \dots, X_p)$, d'où l'expression à l'aide des polynômes symétriques élémentaires des Y_j (voir p. 36) ; puis on prend les coefficients de ce polynôme, ce sont des polynômes symétriques en les X_i à coefficients dans K , et on passe aux polynômes symétriques élémentaires.

Dès lors, les coefficients de M s'expriment rationnellement à l'aide des fonctions symétriques élémentaires des x_i et de celles des y_j , donc ils sont bien dans K .

De même, le produit xy sera racine du polynôme

$$\prod_{\substack{i=1, \dots, p \\ j=1, \dots, q}} (X - x_i y_j)$$

qui est aussi à coefficients dans K .

sont aussi

ou xy , en

thode pour
ne sera pas

m M_x de x
une d'elles
ymétriques
(car elles
que l'on

de M_y . La
pq sommes
ôme

trer que les
que $x + y$

..., y_q) d'un

X_i et toute

symétriques
it d'abord T
 $X_1, \dots, X_r$,
des Y_j (voir
polynômes
polynômes

l'aide des
ls sont bien

Ainsi, $x_1 = \sqrt{2}$ et $y_1 = \sqrt{3}$ sont algébriques sur $\mathbb{Q}$, les polynômes minima sont $X^2 - 2$ et $X^2 - 3$, d'où les autres conjugués respectifs $x_2 = -\sqrt{2}$ et $y_2 = -\sqrt{3}$. Dès lors, $\sqrt{2} + \sqrt{3}$ est racine du polynôme suivant, dont les coefficients sont nécessairement dans $\mathbb{Q}$:

$$M = (X - (\sqrt{2} + \sqrt{3}))(X - (\sqrt{2} - \sqrt{3}))(X - (-\sqrt{2} + \sqrt{3}))(X - (-\sqrt{2} - \sqrt{3}))$$

$$M = (X^2 - (\sqrt{2} + \sqrt{3})^2)(X^2 - (\sqrt{2} - \sqrt{3})^2)$$

$$M = (X^2 - 5 - 2\sqrt{6})(X^2 - 5 + 2\sqrt{6})$$

$$M = (X^2 - 5)^2 - (2\sqrt{6})^2$$

$$M = X^4 - 10X^2 + 1.$$

On avait déjà directement trouvé $\sqrt{2} + \sqrt{3}$ comme racine de ce polynôme (voir p. 81).

Est-ce là le polynôme minimum de $\sqrt{2} + \sqrt{3}$ sur $\mathbb{Q}$? Il faut montrer, soit qu'il est irréductible sur $\mathbb{Q}$, soit que $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ est de degré 4 sur $\mathbb{Q}$.

Or $\sqrt{2} + \sqrt{3}$ est contenu dans $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, qui est de degré 4 car $X^2 - 3$, polynôme minimum de $\sqrt{3}$ sur $\mathbb{Q}$, est irréductible sur $\mathbb{Q}(\sqrt{2})$ (pourquoi?). Dès lors le degré de $\sqrt{2} + \sqrt{3}$ divise 4 et ce n'est ni 1, car $(\sqrt{2} + \sqrt{3})$ n'est pas dans $\mathbb{Q}$, ni 2, car $(\sqrt{2} + \sqrt{3})^2$ n'est pas combinaison $\mathbb{Q}$ -linéaire de 1 et $\sqrt{2} + \sqrt{3}$. Ce degré est donc 4. Conséquences :

- $\sqrt{2} + \sqrt{3}$ est de degré 4 sur $\mathbb{Q}$
- le polynôme $X^4 - 10X^2 + 1$ est le polynôme minimum de $\sqrt{2} + \sqrt{3}$ sur $\mathbb{Q}$, il est irréductible sur $\mathbb{Q}$
- le corps $\mathbb{Q}(\sqrt{2} + \sqrt{3})$, contenu *a priori* dans $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, lui est en fait égal, ce que l'on retrouve directement en écrivant
$$\frac{1}{\sqrt{2} + \sqrt{3}} = \sqrt{3} - \sqrt{2}$$
 et en calculant ainsi $\sqrt{2}$ et $\sqrt{3}$ en fonction de $\sqrt{2} + \sqrt{3}$
- des bases de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ comme $\mathbb{Q}$ -espace sont,

$$\text{soit} \quad (1, \sqrt{2}, \sqrt{3}, \sqrt{6}),$$

$$\text{soit} \quad (1, (\sqrt{2} + \sqrt{3}), (\sqrt{2} + \sqrt{3})^2, (\sqrt{2} + \sqrt{3})^3).$$

Ceci dit, la même méthode appliquée à $x_1 y_1 = \sqrt{6}$ donne le polynôme

$$(X - \sqrt{2}\sqrt{3})(X + \sqrt{2}\sqrt{3})(X + \sqrt{2}\sqrt{3})(X - \sqrt{2}\sqrt{3}),$$

c'est-à-dire $(X^2 - 6)^2$, qui n'est pas ici le polynôme minimum car il est réductible : la somme de $\sqrt{2}$ et $\sqrt{3}$ est de degré 4 mais leur produit est de degré 2.

Le corps des éléments algébriques.

Partons d'un corps K . Les éléments algébriques sur K forment une partie de la clôture algébrique $\bar{K}$ de K (ou de tout corps algébriquement clos contenant K). Or l'opposé et l'inverse d'un élément algébrique non nul sont algébriques, et l'on a montré que la somme et le produit d'éléments algébriques sont encore algébriques.

En conclusion :

L'ensemble des éléments algébriques sur un corps est un corps.

On obtient ainsi une extension A de K , formée par les éléments algébriques sur K . C'est un sous-corps de la clôture algébrique $\bar{K}$, et l'on va montrer qu'il lui est en fait égal : la dernière inclusion de $K \subset A \subset \bar{K}$ est une égalité.

Par construction, A contient toutes les racines des polynômes sur K ; on va voir qu'il contient aussi toutes les racines des polynômes sur A , ce qui entraînera qu'il est algébriquement clos, donc contient la clôture algébrique $\bar{K}$ de K , et finalement lui est égal puisqu'il est contenu dedans.

Soit donc $x \in \bar{K}$ une racine d'un polynôme

$$P = a_0 + a_1 X + \dots + a_n X^n \in A[X].$$

Chaque a_i est algébrique sur K et il faut montrer que x est racine d'un polynôme à coefficients dans K .

Considérons pour cela l'extension $K(a_0, \dots, a_n, x)$. On va prouver qu'elle est de degré fini sur K , ce qui aura pour conséquence le caractère algébrique de x sur K . Par multiplicativité, il suffit de montrer que x est de degré fini sur $K(a_0, \dots, a_n)$, et $K(a_0, \dots, a_n)$ de degré fini sur K . La première affirmation résulte de ce que x est racine de $P \in K(a_0, \dots, a_n)[X]$, la seconde de ce que chaque a_i est algébrique sur K , donc $K(a_0, \dots, a_n)$ de degré fini. Dès lors, x est bien racine d'un polynôme à coefficients dans K , donc il appartient à A .

On peut en tout cas affirmer :

La clôture algébrique d'un corps est une extension algébrique.

Autrement dit, le corps de tous les éléments algébriques sur un corps est sa clôture algébrique. Cette phrase est dangereuse, car on ne précise pas dans quel cadre tout se place : il vaut mieux dire que si C est un corps algébriquement clos contenant K , alors l'ensemble des éléments de C algébriques sur K est la clôture algébrique de K .

LE POLYNÔME

De même, tous les corps précautions :

Ceci dit, la donner explic

sur A dont il

Pour en tr écrit tous les conjugués, c'e

On appelle dans K résult fonctions sym lesquelles sont

Si le corps de complexes racin

De même, une phrase comme « la clôture algébrique d'un corps est l'union de tous les corps de rupture des polynômes sur ce corps » ne peut pas s'avancer sans précautions : dans quel cadre se fait l'union ?

Ceci dit, la méthode ci-dessus est rapide, mais elle a l'inconvénient de ne pas donner explicitement un polynôme *sur* K dont x est racine à partir du polynôme

$$P = a_0 + a_1X + \cdots + a_nX^n$$

sur A dont il est racine.

Pour en trouver un, on va encore « symétriser » à l'aide des conjugués : on écrit *tous* les polynômes obtenus en remplaçant dans P certains des a_i par des conjugués, c'est-à-dire par des racines de leurs polynômes minima.

On appelle T le produit de ces polynômes et le fait que les coefficients de T sont dans K résulte encore du fait qu'ils s'expriment rationnellement à l'aide des fonctions symétriques élémentaires des racines des polynômes minima des a_i , lesquelles sont dans K .

- On a précédemment considéré le réel $x = \sqrt[3]{1 - \sqrt{2}}$ et trouvé qu'il est racine de

$$X^6 - 2X^3 - 1 \in \mathbb{Q}[X].$$

Si l'on applique la méthode ci-dessus, x est algébrique sur $\mathbb{Q}(\sqrt{2})$, de polynôme minimum $X^3 + \sqrt{2} - 1$. Les conjugués de $\sqrt{2}$ sur $\mathbb{Q}$ étant $\sqrt{2}$ et $-\sqrt{2}$, x est racine du polynôme suivant qui doit être à coefficients rationnels :

$$(X^3 - 1 + \sqrt{2})(X^3 - 1 - \sqrt{2}) = (X^3 - 1)^2 - 2.$$

On retrouve bien

$$X^6 - 2X^3 - 1.$$

- De même, si l'on cherche un polynôme sur $\mathbb{Q}$ dont est racine

$$y = \sqrt[3]{1 - \sqrt{2}} + \sqrt{3},$$

on commence par se placer dans $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, d'où le polynôme

$$(X - \sqrt{3})^3 + \sqrt{2} - 1.$$

On écrit ensuite les quatre polynômes obtenus en remplaçant $\sqrt{2}$ et $\sqrt{3}$ par des conjugués (dont eux-mêmes bien sûr...) et on fait leur produit. Le polynôme

$$\begin{aligned} & [(X - \sqrt{3})^3 + \sqrt{2} - 1][(X + \sqrt{3})^3 + \sqrt{2} - 1] \\ & [(X - \sqrt{3})^3 - \sqrt{2} - 1][(X + \sqrt{3})^3 - \sqrt{2} - 1] \end{aligned}$$

s'annule sur y et il doit être à coefficients dans $\mathbb{Q}$. Est-il le polynôme minimum de y sur $\mathbb{Q}$? C'est là un autre problème qui concerne son irréductibilité.

Si le corps de base est $\mathbb{Q}$, les éléments algébriques sur $\mathbb{Q}$ sont les nombres complexes racines d'un polynôme non nul à coefficients entiers. On dit que ce

sont les **nombre algébriques** tout court et leur ensemble forme la clôture algébrique de $\mathbb{Q}$.

Toute expression écrite avec des entiers à l'aide d'opérations rationnelles et d'extractions de radicaux est un nombre algébrique, mais la réciproque est fautive : c'est justement le problème de l'existence d'équations non résolubles par radicaux.

Ainsi, on montrera que c'est le cas de l'équation

$$X^5 - 4X - 2 = 0,$$

ce qui signifie que les racines de $X^5 - 4X - 2$ sont des nombres algébriques non exprimables de cette manière.

Exercices.

1. Si α est dans une extension de K , le corps $K(\alpha^2)$ est toujours contenu dans $K(\alpha)$.

En supposant α algébrique de degré impair, montrer qu'il y a égalité. Réciproque ?

2. Calculer les degrés sur $\mathbb{Q}$ des extensions

$$\mathbb{Q}(\sqrt{3}, \sqrt[4]{2}), \quad \mathbb{Q}(\sqrt{3}, \sqrt{-5}, \sqrt{7}) \quad \text{et} \quad \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}).$$

3. Discuter le degré de $K(\sqrt{x}, \sqrt{y})$ sur K , x et y étant dans K et sans racine carrée dans K ; on montrera que tout dépend de l'existence éventuelle d'une racine carrée de xy dans K .

4. Quel est, sur $\mathbb{Q}$, le degré de

$$\sqrt[3]{\frac{3 + i\sqrt{2}}{1 + \sqrt{5}}} - \sqrt[4]{7}$$

les radicaux ayant le sens usuel de radicaux réels, éventuellement positifs ?

5. Soit u un nombre complexe racine de

$$P = X^3 + X + 1.$$

Trouver un polynôme à coefficients rationnels dont soit racine $v = u^2 + u$ (on pourra calculer les premières puissances de v , et éliminer les puissances de u).

Même question pour $w = u^4 + 1$.

On remplacera ensuite P par $Q = X^4 + 1$, puis par $R = X^4 + X + 1$.

Dans chaque cas, on cherchera aussi les polynômes minimaux.

6. Montrer que le polynôme minimum de $2 \cos \frac{2\pi}{7}$ sur $\mathbb{Q}$ est

$$X^3 + X^2 - 2X - 1.$$

7. Si X est une indéterminée, quel est son polynôme minimum sur

$$\mathbb{Q}\left(\frac{X^2}{X+3}\right)?$$

Les
« adjo
élémen
engend
certain

D'où le

Les élér.

Soit I
 $K(x) \subset$
 α engend
un élém
unique (

Partic
de degré
divise n .
exacteme

Autrer
libre sur

suite (1, 2

L'exis
d'une sui

Une re
est de de

me la clôture

rationnelles et
réciproque est
résolubles par

at des nombres

tenu dans $K(z)$.

té. Réciproque ?

2, $\sqrt[3]{2}$.ans racine carrée
une racine carrée

nt positifs ?

· $v = u^2 + u$ (on
puissances de u).· $X + 1$.

Extensions simples et éléments primitifs

Les premières extensions que l'on a étudiées sont celles que l'on obtient en « adjoignant » un élément à un corps : on part d'un corps K , on prend un élément α dans une extension donnée de K et l'on considère le corps $K(\alpha)$ engendré par K et α . D'autre part, sans être définies sous cette forme brute, certaines extensions s'y ramènent.

Ainsi, l'égalité

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

que l'on a démontrée antérieurement montre qu'un élément bien choisi, $\sqrt{2} + \sqrt{3}$, suffit pour engendrer l'extension, au lieu de deux, $\sqrt{2}$ et $\sqrt{3}$.

D'où les nouvelles notions suivantes.

Les éléments primitifs d'une extension.

Soit L une extension de K . Pour tout élément x de L , on aura l'inclusion $K(x) \subset L$. S'il existe dans L un élément α vérifiant l'égalité $L = K(\alpha)$, on dit que α engendre L sur K , et L s'appelle alors une **extension simple** de K . L'élément α est un **élément primitif** de l'extension L sur K . Il n'a bien sûr aucune raison d'être unique (ainsi $-\alpha$ convient aussi...).

Particulièrement commode est la caractérisation dans le cas d'une extension de degré fini. En effet, si n est le degré de L sur K , le degré de tout élément de L divise n , et les éléments primitifs éventuels sont ceux dont le degré est **exactement** n .

Autrement dit, $z \in L$ est primitif si, et seulement si, la famille $(1, z, \dots, z^{n-1})$ est libre sur K ; il suffit d'ailleurs que, m étant le plus grand diviseur propre de n la suite $(1, z, \dots, z^m)$ soit libre sur K (si n est pair, on prendra $m = \frac{n}{2}$).

L'existence d'éléments primitifs est donc liée à l'existence de bases formées d'une suite finie de puissances d'un élément.

Une remarque avant de voir des exemples : toute extension algébrique simple est de degré fini (égal au degré de tout élément primitif).

Quelques exemples.

- L'extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ est simple, et $\sqrt{2} + \sqrt{3}$ est un élément primitif, comme d'ailleurs tout autre élément de degré 4.
- La clôture algébrique $\mathbb{C}$ de $\mathbb{R}$ est extension simple de $\mathbb{R}$, tout complexe non réel étant élément primitif (car de degré 2).
- La clôture algébrique de $\mathbb{Q}$, ou corps des nombres algébriques, n'est pas extension simple de $\mathbb{Q}$, car c'est une extension algébrique de degré infini.
- Une extension par un radical est une extension simple dont un élément primitif possède une puissance dans le corps de base.
- Si L est une extension de K de degré p premier, c'est une extension simple : en effet, tout élément de $L \setminus K$ a pour degré un diviseur de p autre que 1, ce degré est donc p et tout élément hors de K est primitif. Il n'y a alors aucun corps strictement intermédiaire entre K et L .
- L'élément $x \in K(\alpha, \beta)$ sera primitif si, et seulement si, α et β sont égaux à des fonctions rationnelles en x .

Ainsi, si x et y sont différents dans K , l'égalité

$$\frac{1}{\sqrt{x} + \sqrt{y}} = \frac{\sqrt{x} - \sqrt{y}}{x - y}$$

entraîne

$$2\sqrt{x} = (\sqrt{x} + \sqrt{y}) + \frac{x - y}{(\sqrt{x} + \sqrt{y})}.$$

On en déduit que $\sqrt{x} + \sqrt{y}$ est toujours élément primitif de $K(\sqrt{x}, \sqrt{y})$ (si 2 est non nul dans K , bien sûr).

- Le corps $\mathbb{Q}(\sqrt[3]{2})$ est réel, en prenant pour $\sqrt[3]{2}$ la racine cubique réelle de 2. Donc $X^2 + 1$ est irréductible sur lui et i est de degré 2 sur $\mathbb{Q}(\sqrt[3]{2})$, ce qui montre que l'extension $\mathbb{Q}(\sqrt[3]{2}, i)$ est de degré 6.

Est-elle simple ? Un élément primitif éventuel α sera un élément de degré 6 et il suffira que $(1, \alpha, \alpha^2, \alpha^3)$ soit libre sur $\mathbb{Q}$, car le degré d'un tel α est alors un diviseur de 6 supérieur à 4.

Par analogie avec $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, essayons $z = i + \sqrt[3]{2}$, en étudiant les rationnels a, b, c, d vérifiant

$$a + bz + cz^2 + dz^3 = 0.$$

Calculons donc

$$\begin{aligned} z^2 &= -1 + \sqrt[3]{4} + 2i\sqrt[3]{2} \\ z^3 &= 2 - 3\sqrt[3]{2} + i(3\sqrt[3]{4} - 1). \end{aligned}$$

La nullité de la combinaison ci-dessus entraîne la nullité de sa partie imaginaire, ce qui s'écrit

$$b + 2c\sqrt[3]{2} + d(3\sqrt[3]{4} - 1) = 0.$$

$$(b - d) + 2c\sqrt[3]{2} + 3d\sqrt[3]{4} = 0.$$

Donc $\sqrt[3]{2}$ est racine de

$$(b - d) + 2cX + 3dX^2$$

ce qui exige la nullité de ce polynôme car $\sqrt[3]{2}$ est de degré 3 sur $\mathbb{Q}$. D'où les égalités $d = c = 0$ et $b = d$, qui donnent $a = b = c = d = 0$ et montrent l'indépendance $\mathbb{Q}$ -linéaire de $(1, z, z^2, z^3)$.

En conclusion : z est de degré 6 sur $\mathbb{Q}$ et l'extension $\mathbb{Q}(\sqrt[3]{2}, i)$ est simple, égale à $\mathbb{Q}(\sqrt[3]{2} + i)$. Dès lors, $\sqrt[3]{2}$ et i s'écrivent nécessairement chacun comme polynômes en $\sqrt[3]{2} + i$, de degrés inférieurs à 5, et tout polynôme de degré 6 sur $\mathbb{Q}$ s'annulant en $i + \sqrt[3]{2}$ est irréductible sur $\mathbb{Q}$. On trouve ce polynôme en écrivant par exemple :

$$\begin{aligned}\alpha &= i + \sqrt[3]{2} \\ (\alpha - i)^3 &= 2 \\ \alpha^3 - 3\alpha - 2 &= i(3\alpha^2 - 1) \\ (\alpha^3 - 3\alpha - 2)^2 + (3\alpha^2 - 1)^2 &= 0.\end{aligned}$$

Le polynôme minimum cherché est donc

$$X^6 + 3X^4 - 4X^3 + 3X^2 + 12X + 5.$$

On n'a pas besoin de vérifier son irréductibilité.

• Pour le corps de rupture d'un polynôme de degré 3, on a montré que la différence de deux racines est un élément primitif. On a en effet calculé (voir p. 55), en appelant a, b, c les racines de $X^3 + pX + q$, les égalités

$$a = \frac{3q}{(b - c)^2 + p} \quad \text{et} \quad (b - c)^2 = -3a^2 - 4p.$$

La première montre que $K(b - c)$ contient a , donc aussi $b + c$, donc enfin b et c .

On peut d'ailleurs écrire a sous forme d'un polynôme en $(b - c)$. Il suffit de faire le calcul :

$$\begin{aligned}(b - c)^2 &= -3a^2 - 4p \\ (b - c)^4 &= 9a^4 + 24pa^2 + 16p^2 \\ &= 9(-pa^2 - qa) + 24pa^2 + 16p^2 \\ &= 15pa^2 + 16p^2 - 9qa \\ (b - c)^4 + 5p(b - c)^2 &= -4p^2 - 9qa\end{aligned}$$

$\sqrt{2} + \sqrt{3}$ est un élément de degré 4.

simple de $\mathbb{R}$, tout de degré 2).

mbres algébriques, est une extension

ion simple dont un le corps de base.

premier, c'est une K a pour degré un et tout élément hors corps strictement

lement si, α et β sont

lité

y

$\frac{y}{\sqrt{y}}$.

élément primitif de sûr).

$\sqrt[3]{2}$ la racine cubique qui et i est de degré 2 $\sqrt[3]{2}, i)$ est de degré 6.

el α sera un élément re sur $\mathbb{Q}$, car le degré ur à 4.

$z = i + \sqrt[3]{2}$, en

1).

d'où enfin

$$-9qa = (b - c)^4 + 5p(b - c)^2 + 4p^2.$$

Le problème de l'existence d'un élément primitif.

Dans tous les cas précédents, on a trouvé un élément primitif. Mais est-ce toujours possible ? En d'autres termes, une extension algébrique simple est de degré fini. La réciproque est-elle vraie ?

On va montrer — et c'est un résultat essentiel — que la réponse est « presque toujours » positive. Ce qui revient à montrer l'une des affirmations équivalentes suivantes :

- toute extension de degré fini a un élément primitif ;
- toute extension de degré fini a une base formée de puissances d'un élément ;
- il existe un élément de degré égal au degré de l'extension ;
- tous les éléments sont des polynômes en l'un d'entre eux.

Il y a un cas particulièrement simple, c'est celui où le corps de base K est fini. Car alors une extension L de degré fini sur K est encore finie, et un résultat général affirme que le groupe multiplicatif d'un corps fini est cyclique, c'est-à-dire formé des puissances d'un de ses éléments (appelé générateur). Dès lors, si $\alpha \in L$ est un générateur du groupe multiplicatif $L \setminus \{0\}$, il est clair que l'on a

$$L = K(\alpha).$$

Mais ce résultat concernant les corps finis nous intéresse peu, car il ne comprend ni $\mathbb{Q}$ ni toutes ses extensions.

Ceci dit, il y a des contre-exemples. Ainsi, $\mathbb{Z}/2(X, Y)$ est de degré 4 sur son sous-corps $\mathbb{Z}/2(X^2, Y^2)$, mais chacun de ses éléments est de degré 1 ou 2 sur ce sous-corps : ce n'est pas une extension simple.

Des éléments primitifs d'un corps de rupture.

Bien que l'existence d'éléments primitifs se démontre dans un cadre général d'extension, il est intéressant de faire une démonstration spéciale au cas des corps de rupture. On verra en effet le lien existant entre la recherche d'un élément primitif et les permutations des racines du polynôme : c'est encore cette « vague » notion de conjugué, que l'on précisera plus tard.

Partons donc d'un polynôme $P \in K[X]$, de racines $(x_1, \dots, x_n)$ que l'on pourra supposer simples, quitte à remplacer P par son quotient par le P.G.C.D. de P et P' , ce qui est toujours possible en caractéristique nulle car P' est non nul (voir p. 31).

Tout élément du corps de rupture $K(x_1, \dots, x_n)$ s'écrit

$$z = F(x_1, \dots, x_n)$$

pour un certain polynôme F (pas unique d'ailleurs). A chaque permutation $\sigma \in \Sigma_n$ on va associer le polynôme $\sigma F(X_1, \dots, X_n) = F(X_{\sigma(1)}, \dots, X_{\sigma(n)})$, et l'élément $\sigma z = \sigma F(x_1, \dots, x_n)$ du corps de rupture.

EXTENSIONS

L'idée est la
parcourt Σ_n , pl
manière précise
alors z est élén

En fait, on v
certain sous-gr

Revenons de
indéterminées

Il suffit d'aill
l'identité,

soit différent de

On dira que
($x_1, \dots, x_n$) de

Pour montre
montrer que te

Bien entendu

+ $4p^2$.

L'idée est la suivante : plus les σz auront des valeurs distinctes quand σ parcourt Σ_n , plus z aura de « chance » d'être primitif. On va même démontrer de manière précise que si les σz sont deux à deux distincts quand σ parcourt Σ_n , alors z est élément primitif.

En fait, on verra plus tard qu'il suffit qu'il en soit ainsi quand σ parcourt un certain sous-groupe de Σ_n , qui sera le groupe de Galois de P .

Par exemple, pour

$$P = (X^2 - 2)(X^2 - 3)$$

on vérifie que le polynôme

$$F(X_1, X_2, X_3, X_4) = X_1 + 3X_2 - X_3$$

prend 24 valeurs distinctes sur les 24 combinaisons des racines $(\sqrt{2}, \sqrt{3}, -\sqrt{2}, -\sqrt{3})$. Il en résultera que l'élément

$$F(\sqrt{2}, \sqrt{3}, -\sqrt{2}, -\sqrt{3}) = 2\sqrt{2} + 3\sqrt{3}$$

est élément primitif du corps de rupture de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. On notera que cet élément est aussi la valeur du polynôme $2X_1 + 3X_2$, qui, lui, prend la même valeur si l'on permute les deux dernières racines $-\sqrt{2}$ et $-\sqrt{3}$.

Comme quoi la condition que l'on va démontrer est suffisante mais non nécessaire.

D'ailleurs, on a trouvé comme élément primitif « simple » le nombre $\sqrt{2} + \sqrt{3}$, correspondant à $F = X_1 + X_2$, lequel ne prend que les quatre valeurs distinctes $\pm \sqrt{2} \pm \sqrt{3}$ pour les 24 permutations. Mais c'est qu'en réalité, sur ces 24, seules quatre seront cruciales, les autres « ne compteront pas ». On verra plus tard pourquoi.

Revenons donc à notre problème, et supposons que le polynôme F à n indéterminées vérifie

$$\sigma_1 \neq \sigma_2 \Rightarrow \sigma_1 F(x_1, \dots, x_n) \neq \sigma_2 F(x_1, \dots, x_n).$$

Il suffit d'ailleurs pour cela que, quelle que soit la permutation σ autre que l'identité,

$$\sigma F(x_1, \dots, x_n) = F(x_{\sigma(1)}, \dots, x_{\sigma(n)})$$

soit différent de $F(x_1, \dots, x_n)$.

On dira que F prend $n!$ valeurs distinctes sur les $n!$ permutations des racines $(x_1, \dots, x_n)$ de P .

Pour montrer que l'élément $z = F(x_1, \dots, x_n)$ est alors primitif, il suffit de montrer que tous les x_i sont des polynômes en z , ce qui s'écrit

$$x_i \in K(z).$$

Bien entendu, si on le vérifie pour x_n , il en sera de même pour les autres racines.

Comment démontrer la relation

$$x_n \in K(z) ?$$

On va utiliser pour cela la remarque suivante. Si deux polynômes A et B ont une seule racine commune α (dans un corps contenant les deux corps de rupture), alors α appartient au corps engendré par les coefficients de A et B : en effet, le P.G.C.D. de A et B est $X - \alpha$ (en supposant α racine simple de l'un d'eux), et d'après Bezout il s'écrit $UA + VB$, où U et V sont des polynômes à coefficients dans le corps de ceux de A et B (d'ailleurs $X - \alpha$ se calcule à l'aide d'un algorithme de divisions euclidiennes successives).

Or x_n est racine simple de $P \in K[X] \subset K(z)[X]$. Si l'on trouve un autre polynôme T à coefficients dans $K(z)$ s'annulant en x_n , et pas en $x_1, \dots, x_{n-1}$, on aura bien démontré que x_n est la seule racine commune à P et T, donc appartient à $K(z)$, car ce corps contient les coefficients de P et T.

A cet effet, on va partir du sous-groupe H_n de Σ_n laissant fixe x_n . Ce sous-groupe est isomorphe à Σ_{n-1} et on forme le polynôme à $(n+1)$ indéterminées :

$$R(X, X_1, \dots, X_n) = \prod_{\sigma \in H_n} (X - \sigma F(X_1, \dots, X_n))$$

qui vérifie $R(z, x_1, \dots, x_n) = 0$.

Ce polynôme est symétrique par rapport à $X_1, \dots, X_{n-1}$. Si l'on substitue, à ces indéterminées, les racines $x_1, \dots, x_{n-1}$ de $\frac{P(Y)}{Y - x_n} \in K(x_n)[Y]$, il restera donc un polynôme en X et x_n , soit

$$R(X, x_1, \dots, x_n) = S(X, x_n).$$

C'est là le résultat de la substitution de Y par x_n dans un polynôme $S(X, Y)$. Mais $S(z, Y)$ est un polynôme $T(Y)$ nul pour $Y = x_n$, car $S(z, x_n)$ est égal à $R(z, x_1, \dots, x_n) = 0$; de plus T a ses coefficients dans $K(z)$. Il suffit alors de montrer que T ne s'annule pas en $x_1, \dots, x_{n-1}$. Bornons-nous à prouver $T(x_1) \neq 0$, ce qui s'écrit

$$S(z, x_1) \neq 0.$$

Or $S(z, x_1)$ est la valeur de R en $(z, x_n, x_2, \dots, x_{n-1}, x_1)$ au lieu de $(z, x_1, \dots, x_n)$; si l'on appelle τ la transposition qui échange 1 et n, on trouve

$$T(x_1) = \prod_{\sigma \in H_n} (z - \sigma \tau F(x_1, \dots, x_n))$$

Ici intervient l'hypothèse : $z = F(x_1, \dots, x_n)$ n'est égal à aucun des $\sigma \tau F(x_1, \dots, x_n)$, car aucun des $\sigma \tau$ n'est l'identité.

En conclusion : les polynômes P et T n'ont que x_n comme racine commune, leurs coefficients sont dans K et $K(z)$ respectivement, donc x_n est dans $K(z)$.

Rappelons que notre corps de base K contient $\mathbb{Q}$ (nécessaire pour être sûr que l'on peut supposer les racines simples). Trouver un polynôme F tel que $F(x_1, \dots, x_n)$ soit différent de $F(x_{\sigma(1)}, \dots, x_{\sigma(n)})$ pour tout $\sigma \in \Sigma_n$ (id est facile. Il suffit de trouver des $\lambda_1, \dots, \lambda_n$ dans K tels que l'on ait

$$\sigma \neq \text{id} \Rightarrow \lambda_{\sigma(1)}x_1 + \dots + \lambda_{\sigma(n)}x_n \neq \lambda_1x_1 + \dots + \lambda_nx_n.$$

Et c'est possible pour les λ_i . On peut choisir $\mathbb{Q}$, ou

Le théorème de

Ceci dit, en réalité c'est vrai dans le

Il suffit de trouver K (on ne suppose pas que $z \in K(x, y)$ vérifie

La démarche

des polynômes tout à l'heure sera clairement plus

On va montrer

soit élément principal clôture algébrique

• il existe $t \in K$ tel que $i = 1, \dots, p$ et j

• l'élément $t \in K$

est y (on a posé

• l'élément y a des coefficients dans

• de même x

On a donc montré qu'il existe dans $K(\alpha_1,$

Et c'est possible car σ décrit un ensemble fini, alors que l'on a un choix infini pour les λ_i . On peut même prendre les λ_i dans $\mathbb{Q}$ ou dans $\mathbb{Z}$. Pour un corps contenant $\mathbb{Q}$, on a démontré :

Tout corps de rupture est une extension simple, et il y a un élément primitif combinaison linéaire à coefficients entiers des racines du polynôme.

Le théorème de l'élément primitif.

Ceci dit, en restant en caractéristique nulle, le théorème de l'élément primitif est vrai dans le cas général.

Toute extension de degré fini est simple.

Il suffit de trouver un élément primitif à $K(x, y)$, où x et y sont algébriques sur K (on ne suppose pas ici que $K(x, y)$ soit un corps de rupture), donc de trouver un $z \in K(x, y)$ vérifiant

$$x \in K(z) \quad \text{et} \quad y \in K(z).$$

La démarche est semblable, en introduisant les racines

$$(x = x_1, x_2, \dots, x_p) \quad \text{et} \quad (y = y_1, y_2, \dots, y_q)$$

des polynômes minima M_x et M_y de x et y sur K . Le rôle des « conjugués » de tout à l'heure sera ici tenu en remplaçant x et y par les x_i et les y_j , le lien apparaîtra clairement plus loin (voir p. 164).

On va montrer qu'il existe $t \in K$ tel que

$$z = x + ty$$

soit élément primitif. Pour cela, on vérifie successivement (en se plaçant dans une clôture algébrique de K ou dans le corps de rupture de $M_x M_y$) :

- il existe $t \in K$ tel que les éléments $x_i + ty_j$ soient deux à deux distincts, pour $i = 1, \dots, p$ et $j = 1, \dots, q$ (on se sert du fait que K est infini);

- l'élément t étant ainsi choisi, la seule racine commune des polynômes

$$M_y(X) \quad \text{et} \quad M_x(z - tX)$$

est y (on a posé $z = x + ty$);

- l'élément y appartient à $K(z)$, car $X - y$ est le P.G.C.D. de deux polynômes à coefficients dans $K(z)$;

- de même x est dans $K(z)$, d'où l'égalité

$$K(z) = K(x, y).$$

On a donc montré plus précisément que, si les α_i sont algébriques sur K , il existe dans $K(\alpha_1, \dots, \alpha_n)$ un élément primitif combinaison K -linéaire des α_i (on

peut même trouver une combinaison $\mathbb{Z}$ -linéaire). Ce résultat inclut bien sûr celui concernant les corps de rupture.

Le théorème de l'élément primitif est d'importance essentielle, tant en théorie qu'en pratique.

Premiers exemples.

- Le fait que $\sqrt{2} + \sqrt{3}$ est élément primitif de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ résulte de ce que les quatre éléments suivants sont distincts :

$$\sqrt{2} + \sqrt{3}, \quad \sqrt{2} - \sqrt{3}, \quad -\sqrt{2} + \sqrt{3}, \quad -\sqrt{2} - \sqrt{3}.$$

- De même, pour $\mathbb{Q}(i, \sqrt[3]{2})$, les racines de $X^2 + 1$ sont i et $-i$, celles de $X^3 - 2$ sont $\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}$, et les six éléments suivants sont deux à deux distincts :

$$\begin{array}{lll} i + \sqrt[3]{2}, & -i + \sqrt[3]{2}, & i + j\sqrt[3]{2}, \\ -i + j\sqrt[3]{2}, & i + j^2\sqrt[3]{2}, & -i + j^2\sqrt[3]{2}. \end{array}$$

Donc $i + \sqrt[3]{2}$ est élément primitif de $\mathbb{Q}(i, \sqrt[3]{2})$, comme on l'a montré directement en calculant son degré (voir p. 103).

- Si l'on part de $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, on l'écrira d'abord $\mathbb{Q}(\sqrt{2} + \sqrt{3}, \sqrt{5})$ et l'élément $\sqrt{2} + \sqrt{3} + \sqrt{5}$ est primitif car les huit éléments $\pm \sqrt{2} \pm \sqrt{3} \pm \sqrt{5}$ sont deux à deux distincts.

On utilise le fait que $X^2 - 5$ est irréductible sur $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, et que les racines du polynôme minimum de $\sqrt{2} + \sqrt{3}$ sur $\mathbb{Q}$ sont $\pm \sqrt{2} \pm \sqrt{3}$.

- L'extension $\mathbb{Q}(i, \sqrt{3})$ est une extension par radicaux successifs. Mais en fait, $i + \sqrt{3}$ est primitif et un calcul simple donne $(i + \sqrt{3})^3 = 8i$, ce qui prouve qu'il existe un élément primitif dont la puissance sixième est égale à -64 .

Donc $\mathbb{Q}(i, \sqrt{3})$ est même une extension par radical, engendrée par une racine de $X^6 + 64$.

Un calcul d'élément primitif.

Prenons un polynôme pair de degré 4 sur $\mathbb{Q}$, soit $X^4 + aX^2 + b$, et supposons-le irréductible. Les quatre racines s'écrivent $(\alpha_1, \alpha_2, -\alpha_1, -\alpha_2)$, avec

$$\alpha_1^2 + \alpha_2^2 = -a \quad \text{et} \quad \alpha_1^2 \alpha_2^2 = b;$$

le corps de rupture est $\mathbb{Q}(\alpha_1, \alpha_2)$, de degré 4 ou 8 suivant que α_2

appartient ou non à $\mathbb{Q}(\alpha_1)$ (son carré y appartient toujours, d'après la relation $\alpha_1^2 + \alpha_2^2 = -a$). Les deux cas peuvent se produire. Par exemple

- $X^4 - 10X^2 + 1$: le corps de rupture est

$$\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}), \text{ de degré } 4.$$

- $X^4 - 2$: le corps de rupture est $\mathbb{Q}(\sqrt[4]{2}, i)$, où $\sqrt[4]{2}$ est la racine quatrième réelle positive de 2, et il est de degré 8 par multiplicativité.

La somme $s = \alpha_1 + \alpha_2$ de deux éléments engendrant le corps de rupture vérifie

$$s^2 = \alpha_1^2 + \alpha_2^2 + 2\alpha_1\alpha_2$$

d'où

$$s^2 + a = 2\alpha_1\alpha_2$$

et

$$(s^2 + a)^2 - 4b = 0$$

ce qui montre qu'elle est de degré 4 au plus, donc en tout cas elle n'est *pas* élément primitif du corps de rupture $\mathbb{Q}(\alpha_1, \alpha_2)$ dans le second cas (dans notre exemple, on trouve $s = (1 + i)\sqrt[4]{2}$, dont la puissance quatrième vaut -8). Ceci dit, d'après le théorème de l'élément primitif, il doit exister un élément primitif de la forme $\alpha_1 + q\alpha_2$ pour un certain rationnel q (forcément différent de 1 dans le second cas, et aussi de -1 d'ailleurs).

Si l'on essaie $q = 2$, on pose $u = \alpha_1 + 2\alpha_2$ et le problème revient à montrer que α_1 ou α_2 (l'un des deux suffit) est égal à un polynôme en u : on aura bien alors

$$\mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\alpha_1 + 2\alpha_2).$$

Pour ce faire, on peut calculer :

$$\begin{aligned} u &= \alpha_1 + 2\alpha_2 \\ u^2 &= \alpha_1^2 + 4\alpha_2^2 + 4\alpha_1\alpha_2 \\ u^2 + 3\alpha_1^2 &= -4a + 4\alpha_1\alpha_2 \\ (u^2 + 3\alpha_1^2)^2 &= 16(\alpha_1\alpha_2 - a)^2. \end{aligned}$$

On développe cette dernière égalité en remplaçant $9\alpha_1^4$ par $-9a\alpha_1^2 - 9b$ et $(\alpha_1\alpha_2)^2$ par b et il reste

$$u^4 - 25b - 16a^2 = 3\alpha_1^2(3a - 2u^2) - 32a\alpha_1\alpha_2.$$

En comparant à

$$u^2 + 4a = -3\alpha_1^2 + 4\alpha_1\alpha_2$$

on en déduit α_1^2 et $\alpha_1\alpha_2$ en fonction de u dès que $3a - 2u^2 - 8a$ est non nul, ce qui s'écrit

$$2u^2 + 5a \neq 0.$$

Dans ces conditions, α_1^2 et $\alpha_1\alpha_2$ sont dans $\mathbb{Q}(u)$, donc aussi leur quotient $\frac{\alpha_1}{\alpha_2}$, ce qui, joint à l'égalité $\alpha_1 + 2\alpha_2 = u$, donne bien α_1 et α_2 dans $\mathbb{Q}(u)$.

Reste à montrer que l'hypothèse $2u^2 + 5a = 0$ est impossible, et pour cela à trouver une contradiction avec l'irréductibilité de $X^4 + aX^2 + b$. L'égalité

$$2(\alpha_1 + 2\alpha_2)^2 + 5a = 0$$

donne $3a + 6\alpha_1^2 = 8\alpha_1\alpha_2$ que l'on élève au carré. En tenant compte de $(\alpha_1\alpha_2)^2 = b$, il reste

$$36\alpha_1^4 + 36a\alpha_1^2 + 9a^2 - 64b = 0.$$

Comme le polynôme *minimum* de α_1 est $X^4 + aX^2 + b$, on doit avoir

$$9a^2 - 64b = 36b$$

d'où $9a^2 = 100b$. Mais l'égalité

$$X^4 + aX^2 + \frac{9a^2}{100} = \left(X^2 + \frac{a}{10}\right)\left(X^2 + \frac{9a}{10}\right)$$

montre que le polynôme serait alors réductible : contradiction.

En conclusion, si

$$X^4 + aX^2 + b$$

est irréductible et si α_1 et α_2 sont deux racines non opposées, alors $\alpha_1 + 2\alpha_2$ est *toujours* élément primitif du corps de rupture.

Les corps intermédiaires d'une extension simple.

Un corps intermédiaire entre un corps K et une extension L est un corps A vérifiant $K \subset A \subset L$. Si les deux inclusions sont strictes, on dit que A est *strictement* intermédiaire entre K et L ; quand le degré de L sur K est fini, le degré de A sur K est alors un diviseur propre de $(L : K)$ autre que 1.

- Le corps $\mathbb{R}$ est strictement intermédiaire entre $\mathbb{Q}$ et $\mathbb{C}$.
- Il n'y a pas de corps strictement intermédiaire entre $\mathbb{R}$ et $\mathbb{C}$.
- Plus généralement, il n'y a pas de corps strictement intermédiaire entre un corps K et une extension L de degré un nombre premier (si $L : K$ est premier, il n'a aucun diviseur propre autre que 1); une telle extension L est une extension propre minimale de K .
- Le corps $\mathbb{Q}(\sqrt[3]{2})$ est strictement intermédiaire entre $\mathbb{Q}$ et $\mathbb{Q}(\sqrt[3]{2})$.

EXTEN

Que
algébrique
appeler

Si A

• le
• le
dans K
• le
de α su.

Des
appeler
dans A ,

Pour
et sur B .
 α a mêm
irréducti
minimu

Dans
les coeff
sur K . C
fini de c
décomp.

On a r
primitif
une exte

coefficier

devra av
cherché).

Quelques

u), donc aussi leur
 $= u$, donne bien α_1

0 est impossible, et
 l'irréductibilité de

un carré. En tenant

$= 0$.

$-aX^2 + b$, on doit

$$X^2 + \frac{9a}{10}$$

ble : contradiction.

non opposées, alors
 corps de rupture.

on L est un corps A
 ; on dit que A est
 sur K est fini, le degré
 ue 1.

entre $\mathbb{Q}$ et $\mathbb{C}$.

liaire entre $\mathbb{R}$ et $\mathbb{C}$.

corps strictement
 ision L de degré un
 aucun diviseur propre
 e extension propre

édiaire entre $\mathbb{Q}$ et

Que peut-on dire des corps intermédiaires entre un corps et une extension algébrique simple ? Partons d'un corps K , et d'un élément α algébrique sur K , et appelons M_α le polynôme minimum de α sur K .

Si A est un corps intermédiaire entre K et $K(\alpha)$, on notera successivement :

- le corps $A(\alpha)$ est égal à $K(\alpha)$;
- le polynôme minimum M_A de α sur A divise M_α dans $A[X]$, donc *a fortiori* dans $K(\alpha)[X]$;
- le corps A est engendré sur K par les coefficients du polynôme minimum M_A de α sur A .

Des trois points, seul le dernier n'est pas évident. Pour le prouver, on va appeler B le corps engendré sur K par les coefficients de M_A . Ces coefficients étant dans A , il en est de même de tous les éléments de B , d'où la chaîne

$$K \subset B \subset A \subset K(\alpha).$$

Pour montrer l'égalité $B = A$, il suffit de vérifier que $K(\alpha)$ a même degré sur A et sur B . Mais $K(\alpha)$ est aussi égal à $A(\alpha)$ et à $B(\alpha)$, donc tout revient à prouver que α a même degré sur A et sur B . Or son polynôme minimum M_A sur A est irréductible *a fortiori* sur B (car B est inclus dans A), c'est donc aussi le polynôme minimum sur B , d'où l'égalité des degrés.

Dans ces conditions, tout corps intermédiaire entre K et $K(\alpha)$ est engendré par les coefficients d'un diviseur, dans $K(\alpha)[X]$, du polynôme minimum M_α de α sur K . Or, à des facteurs constants près, un polynôme donné n'a qu'un nombre fini de diviseurs dans un anneau de polynômes sur un corps (à cause de la décomposition en facteurs premiers, par exemple). D'où le résultat :

Entre un corps et une extension algébrique simple, il n'y a qu'un nombre fini de corps intermédiaires.

On a même un moyen de chercher ces corps intermédiaires : si α est un élément primitif de degré n et de polynôme minimum M_α , alors, pour un diviseur m de n , une extension de degré m intermédiaire entre K et $K(\alpha)$ est engendrée par les coefficients d'un certain diviseur, de degré $\frac{n}{m}$, de M_α dans $K(\alpha)[X]$; ce diviseur devra avoir α pour racine (car c'est le polynôme minimum de α sur le corps cherché), et avoir bien sûr ses coefficients dans $K(\alpha)$.

Quelques exemples.

- Soit $x = \sqrt[4]{2}$ la racine quatrième réelle positive de 2. Le polynôme $X^4 - 2$ étant irréductible sur $\mathbb{Q}$ (pourquoi ?), l'extension simple $\mathbb{Q}(x)$ est de degré 4.

Un éventuel corps strictement intermédiaire entre $\mathbb{Q}$ et $\mathbb{Q}(x)$ sera de degré 2 et correspondra à un diviseur de degré 2 de $X^4 - 2$ dans $\mathbb{Q}(x)[X]$ s'annulant en $\sqrt[4]{2}$.

Tout corps strictement intermédiaire entre $\mathbb{Q}$ et $\mathbb{Q}(i, \sqrt[3]{2})$ est de degré 2 ou 3.

Un corps intermédiaire de degré 3 est engendré par les coefficients d'un diviseur de degré 2 de M dans $\mathbb{Q}(i, \sqrt[3]{2})[X]$, ayant $i + \sqrt[3]{2}$ pour racine et ses coefficients dans $\mathbb{Q}(i, \sqrt[3]{2})$. Les cinq candidats possibles sont

$$(X - i - \sqrt[3]{2})(X + i - \sqrt[3]{2}), \quad (X - i - \sqrt[3]{2})(X \pm i - j\sqrt[3]{2}), \\ (X - i - \sqrt[3]{2})(X \pm i - j^2\sqrt[3]{2}).$$

Les quatre derniers ont un terme constant hors de $\mathbb{Q}(i, \sqrt[3]{2})$, à cause de la présence de j ou j^2 . Seul reste le premier, égal à

$$(X - \sqrt[3]{2})^2 + 1 = X^2 - 2\sqrt[3]{2}X + \sqrt[3]{4} + 1,$$

qui donne, comme seul corps intermédiaire de degré 3, le corps $\mathbb{Q}(\sqrt[3]{2})$ engendré par ses coefficients.

Quant aux corps intermédiaires de degré 2, ils seront donnés par les diviseurs de degré 3 de M , ayant toujours $i + \sqrt[3]{2}$ pour racine et des coefficients dans $\mathbb{Q}(i, \sqrt[3]{2})$. La décomposition

$$M = (X^3 - 3iX^2 - 3X - 2 + i)(X^3 + 3iX^2 - 3X - 2 - i)$$

donne le corps intermédiaire $\mathbb{Q}(i)$.

Une remarque.

On a montré que pour une extension simple algébrique, il n'y a qu'un nombre fini de corps intermédiaires. On montre, dans le cas d'un corps *infini*, la réciproque :

Si une extension de degré fini n'a qu'un nombre fini de corps intermédiaires, elle est simple.

C'est d'ailleurs là une seconde méthode de démonstration du théorème de l'élément primitif, mais elle suppose l'étude *a priori* des corps intermédiaires d'une extension de degré fini.

En fait, l'idée est toujours la même : on part du corps infini K , et des éléments algébriques α et β tels qu'il n'y ait qu'un nombre fini de corps intermédiaires entre K et $K(\alpha, \beta)$. Pour montrer l'existence d'un élément primitif, on remarque que, pour tout $t \in K$, le corps $K(\alpha + t\beta)$ est intermédiaire ; comme K est infini, il existe t et u différents dans K avec

$$K(\alpha + t\beta) = K(\alpha + u\beta).$$

Ce corps intermédiaire contient $\alpha + t\beta$ et $\alpha + u\beta$, donc il contient leur différence $(t - u)\beta$ et par suite il contient β et aussi α : on a bien prouvé que cet $\alpha + t\beta$ est alors élément primitif.

Exercices.

1. Si X et Y sont des indéterminées, l'extension $K(X, Y)$ est-elle simple ?
2. Montrer que $\sqrt{2} + \sqrt[3]{2}$ est élément primitif de $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$, de même que $\sqrt{5} + \sqrt[3]{2}$ pour $\mathbb{Q}(\sqrt[3]{2}, \sqrt{5})$.
Dans les deux cas, calculer le degré, donner plusieurs bases, et trouver les corps intermédiaires.
3. Étudier les corps intermédiaires pour $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ sur $\mathbb{Q}$. Caractériser tous les éléments primitifs.
4. Étudier les corps intermédiaires de $K(\sqrt{x}, \sqrt{y})$ sur K .
5. Si K_1 et K_2 sont des corps intermédiaires entre K et H et si $K_1 : K$ et $K_2 : K$ sont premiers entre eux, montrer que l'on a

$$K_1 \cap K_2 = K.$$

6. Soit $\mathbb{Z}/2(X, Y)$ le corps des fractions rationnelles à deux indéterminées sur $\mathbb{Z}/2$. Montrer que son degré sur $\mathbb{Z}/2(X^2, Y^2)$ est 4 et que le carré de tout élément du premier est dans le second. Prouver que l'extension n'est pas simple en montrant l'existence d'une infinité de corps intermédiaires.

En considérant $\mathbb{Z}/2(X, Y)$ comme corps de rupture sur $\mathbb{Z}/2(X^2, Y^2)$ de

$$P(Z) = (Z^2 - X^2)(Z^2 - Y^2),$$

examiner « où le bât blesse » dans la démonstration des éléments primitifs d'un corps de rupture.

7. Donner des exemples d'extensions telles que les corps intermédiaires soient totalement ordonnés par inclusion.
8. On a montré que $x = i + \sqrt[3]{2}$ est élément primitif de $\mathbb{Q}(i, \sqrt[3]{2})$. Exprimer i et $\sqrt[3]{2}$ comme des polynômes en x .
9. Les éléments primitifs du corps $K(X)$ des fractions rationnelles sur K sont les fractions

$$\frac{aX + b}{cX + d}$$

avec $ad - bc \neq 0$.

10. On dit qu'une extension de K admet une base normale s'il existe un élément primitif tel que la famille des conjugués soit linéairement indépendante sur K . Trouver des bases normales pour les exemples classiques, comme

$$\mathbb{Q}(\sqrt{2}), \quad \mathbb{Q}(\sqrt[3]{2}), \quad \mathbb{Q}(\sqrt{2}, \sqrt{3}), \quad \mathbb{Q}(i, \sqrt[3]{2}), \dots$$

11. Pour montrer que toute extension de degré fini d'un corps fini est simple, on a utilisé le résultat suivant : le groupe multiplicatif d'un corps fini est cyclique.

Dér.
grou
enti
• pe

• er
divis

• l'e
p^m
• l'e
• to
• l'e
• les
• to
• K'

12. Une
« for
deux
degré

où l'

Ceci

et pou
 $\alpha_{i1} =$
Mont

soient
Pour

est él
comm

A tout
dans u
formu
sur λ_1
symétr
le corp

Démontrons-le, en partant d'un corps fini K et en appelant n le cardinal de son groupe multiplicatif $K^* = K \setminus \{0\}$. A tout $x \in K^*$ on associe son ordre $\sigma(x)$, plus petit entier > 0 tel que $x^{\sigma(x)} = 1$. On vérifie successivement :

- pour tout $x \in K^*$ et tout $s \in \mathbb{Z}$

$$x^s = 1 \Leftrightarrow \sigma(x) \mid s;$$

- en appelant z un élément d'ordre m maximum et x un élément dont l'ordre ne divise pas m , il existe p premier, q et m' premiers avec p , et deux entiers α et β avec

$$m = p^\beta m', \quad \sigma(x) = p^\alpha q, \quad \beta < \alpha;$$

- l'élément x^q est d'ordre p^α , l'élément z^{p^β} est d'ordre m' , et leur produit est d'ordre $p^\alpha m' > m$;
- l'ordre de tout élément de K^* divise l'ordre maximum $m = \sigma(z)$;
- tout élément de K^* est racine de $X^m - 1$;
- l'entier m est égal à n ;
- les puissances $z, z^2, \dots, z^n$ sont deux à deux distinctes;
- tout élément de K^* est puissance de z ;
- K^* est un groupe cyclique, engendré par z .

12. Une démonstration plus « directe » du théorème de l'élément primitif utilise la « formule d'interpolation de Lagrange » : si $x_1, \dots, x_{n+1}$ et $y_1, \dots, y_{n+1}$ sont deux familles d'éléments de K deux à deux distincts, le seul polynôme sur K de degré n prenant la valeur y_i au point x_i est

$$\sum_{i=1}^{n+1} \frac{T(X)}{X - x_i} \frac{y_i}{T'(x_i)}$$

où l'on a posé

$$T(X) = \prod_{i=1}^{n+1} (X - x_i).$$

Ceci dit, partons de l'extension algébrique

$$K(\alpha_1, \dots, \alpha_p)$$

et pour tout i appelons $\alpha_{i1}, \dots, \alpha_{i\sigma(i)}$ les racines du polynôme minimum de α_i (avec $\alpha_{i1} = \alpha_i$).

Montrer qu'il existe $\lambda_1, \dots, \lambda_p$ dans K tels que les éléments

$$\lambda_1 \alpha_{1i_1} + \lambda_2 \alpha_{2i_2} + \dots + \lambda_p \alpha_{pi_p}$$

soient deux à deux distincts, quand $i_1, \dots, i_p$ prennent toutes les valeurs possibles. Pour vérifier que

$$\beta = \lambda_1 \alpha_1 + \lambda_2 \alpha_2 + \dots + \lambda_p \alpha_p$$

est élément primitif de $K(\alpha_1, \dots, \alpha_p)$, il suffit d'écrire tout $\theta \in K(\alpha_1, \dots, \alpha_p)$ comme un polynôme en β à coefficients dans K .

A toute suite $i_1, \dots, i_p$ correspond un élément $\theta(i_1, \dots, i_p)$, obtenu en remplaçant, dans une expression donnée de θ , α_1 par α_{1i_1} , α_2 par α_{2i_2} , $\dots$. Puis on écrira, par la formule d'interpolation de Lagrange, le polynôme prenant la valeur $\theta(i_1, \dots, i_p)$ sur $\lambda_1 \alpha_{1i_1} + \dots + \lambda_p \alpha_{pi_p}$. On montrera que ses coefficients sont des fonctions symétriques par rapport aux racines des polynômes minima des α_i , donc sont dans le corps K . Quel est le degré de ce polynôme ? Quelle est sa valeur en β ?

Dans le cas du corps de rupture de $P \in K[X]$, il suffit que les n ! expressions

$$\lambda_1 t_{\sigma(1)} + \cdots + \lambda_n t_{\sigma(n)}$$

soient deux à deux distinctes (n est le degré de P , $t_1, \dots, t_n$ sont les racines de P , toutes simples, et σ décrit le groupe Σ_n des permutations).

Application : montrer que $i + \sqrt[3]{2}$ est élément primitif de $\mathbb{Q}(i, \sqrt[3]{2})$ et retrouver par Lagrange l'expression de i comme polynôme en $i + \sqrt[3]{2}$.

En gr
à $K \llcorner \overline{K}$
P ». Il r
extensio
rupture,
Ceci d
de K , a
 $K(x_1, \dots$
On peut
les racine

Rappel d

s n ! expressions

nt les racines de P,

$\sqrt[3]{2}$) et retrouver par

Quelques corps de rupture

En gros, le corps de rupture d'un polynôme $P \in K[X]$ s'obtient en adjoignant à K « le minimum pour pouvoir exprimer rationnellement toutes les racines de P ». Il ne faut pas oublier cette propriété de minimum : si l'on trouve une extension L de K qui contient toutes les racines de P , elle contient le corps de rupture, mais l'inclusion peut être stricte si L est « trop grand ».

Ceci dit, si $(x_1, \dots, x_n)$ est la famille des racines de P dans la clôture algébrique de K , alors le corps de rupture de P est $K(x_1, \dots, x_n)$; il s'écrit d'ailleurs $K(x_1, \dots, x_{n-1})$, car la somme de la famille des racines est dans le corps de base K . On peut bien sûr aussi utiliser les factorisations éventuelles de P et ôter de la liste les racines de P qui sont dans K .

Rappel de quelques exemples classiques.

- Le corps de rupture de

$$X^2 + sX + t \in K[X]$$

s'obtient par adjonction d'une racine carrée du discriminant, c'est $K(\sqrt{s^2 - 4t})$, extension simple de degré 1 ou 2 (on suppose ici car $K \neq 2$) suivant que le polynôme est réductible ou non sur K , donc que $s^2 - 4t$ est ou n'est pas un carré dans K .

- Le corps de rupture de $X^3 - 1$ sur $\mathbb{Q}$ est aussi celui de

$$\frac{X^3 - 1}{X - 1} = X^2 + X + 1.$$

C'est donc $\mathbb{Q}(\sqrt{-3})$, les racines étant

$$1, j = \frac{-1 + i\sqrt{3}}{2} \quad \text{et} \quad j^2 = \frac{-1 - i\sqrt{3}}{2}.$$

- Pour $X^3 - 2$ sur $\mathbb{Q}$, on doit adjoindre une racine cubique de 2, par exemple la réelle, notée $\sqrt[3]{2}$, et aussi j , car les deux autres sont alors $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$. Le corps de rupture est $(\mathbb{Q}\sqrt[3]{2}, j) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$, de degré 6 : en effet, $X^2 + 3$ est irréductible sur $\mathbb{Q}(\sqrt[3]{2})$, donc $\sqrt{-3}$ est de degré 2 sur $\mathbb{Q}(\sqrt[3]{2})$, et

$\sqrt[3]{2}$ de degré 3 sur $\mathbb{Q}$. On vérifie que $\sqrt[3]{2} + \sqrt{-3}$ est de degré 6 sur $\mathbb{Q}$, il est élément primitif et l'extension est simple. Les deux familles

$$1, \sqrt[3]{2}, \sqrt[3]{4}, i\sqrt[3]{2}, i\sqrt[3]{4}, \sqrt[3]{2}\sqrt[3]{3}, i\sqrt[3]{4}\sqrt[3]{3}$$

et

$1, \sqrt[3]{2} + i\sqrt[3]{3}, (\sqrt[3]{2} + i\sqrt[3]{3})^2, (\sqrt[3]{2} + i\sqrt[3]{3})^3, (\sqrt[3]{2} + i\sqrt[3]{3})^4, (\sqrt[3]{2} + i\sqrt[3]{3})^5$
sont toutes deux bases du corps de rupture sur $\mathbb{Q}$.

• Pour $X^4 - 2$ sur $\mathbb{Q}$, on note $\sqrt[4]{2}$ la racine quatrième réelle positive de 2; les quatre racines du polynôme sont alors

$$\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2} \text{ et } -i\sqrt[4]{2}.$$

Le corps de rupture est donc $\mathbb{Q}(\sqrt[4]{2}, i)$, de degré 8 car $X^2 + 1$ est irréductible sur le corps réel $\mathbb{Q}(\sqrt[4]{2})$, et $X^4 - 2$ est irréductible sur $\mathbb{Q}$.

Ici encore, on montre que $i + \sqrt[4]{2}$ est élément primitif.

• Pour le polynôme

$$X^3 + pX + q \in K[X]$$

on a vu que le corps de rupture est engendré par la différence de deux racines. Les formules de Cardan (voir p. 59) montrent aussi que les racines sont dans le corps obtenu en adjoignant successivement j (donc $\sqrt{-3}$), puis une racine carrée de

$$27(4p^3 + 27q^2) = -3 \times 3^2 \times (-4p^3 - 27q^2),$$

c'est-à-dire une racine carrée de $\Delta = -4p^3 - 27q^2$, et enfin une racine cubique de

$$z = \frac{-27q + 3\sqrt{-3}\sqrt{\Delta}}{2}.$$

Le corps de rupture est donc contenu dans $K(\sqrt{-3}, \sqrt{\Delta}, \sqrt[3]{z})$, mais ceci ne prouve pas qu'il lui soit égal (prendre l'exemple de X^3 , celui de $X^3 - X$).

• Le polynôme $1 + X + X^2 + X^3$ sur $\mathbb{Q}$ a pour racine -1 , son quotient par $X + 1$ est $1 + X^2$, donc son corps de rupture est $\mathbb{Q}(i)$.

Les extensions quadratiques.

Le corps de rupture sur K d'un polynôme de degré 2 irréductible est une extension de degré 2 de K (on suppose toujours ici $\text{car } K \neq 2$). Il est facile de

QUELQ

voir que
est de d

et L est

On a
sont à la

• les co
• les ex
élément
écrire q

Toute
En pa
et 1 sont
quadrati
extensio

Sur le de

Si P es
sur le cor
Appelc
 $K(x_1, \dots$
produit d
D'où 1
 $K(x_1, \dots$

On peu

on trouve

Pour a
qu'une fo
de P ; l'en
rupture es
du degré
Or

a_1 est r

a_2 est r

a_3 est r

st de degré 6
le. Les deux

voir que la réciproque est vraie : si L est de degré 2 sur K , on prend $x \in L \setminus K$ qui est de degré 2 sur K , d'où l'égalité

$$L = K(x)$$

et L est corps de rupture du polynôme minimum de x sur K .

On appelle **extension quadratique** une extension de degré 2. Ces extensions sont à la fois :

- les corps de rupture de polynômes irréductibles de degré 2 ;
- les extensions par racine carrée, c'est-à-dire obtenues par adjonction d'un élément hors du corps de base mais dont le carré est dans ce corps (plus long à écrire qu'à saisir...).

Toutes ces notions sont équivalentes.

En particulier, les nombres constructibles à la règle et au compas à partir de 0 et 1 sont ceux qui appartiennent aux extensions de $\mathbb{Q}$ obtenues par extensions quadratiques successives. Le corps de ces nombres constructibles est sans extension quadratique propre, tous les polynômes de degré 2 y sont réductibles.

Sur le degré du corps de rupture.

Si P est un polynôme de degré n , chaque racine de P est de degré inférieur à n sur le corps de base K .

Appelons $(x_1, \dots, x_n)$ la famille des racines de P . Le corps de rupture est alors $K(x_1, \dots, x_n)$, c'est une extension algébrique dont le degré est inférieur au produit des degrés, donc inférieur *a fortiori* à n^n .

D'où la première majoration, grossière, du degré du corps de rupture $K(x_1, \dots, x_n) = L$:

$$L : K \leq n^n.$$

On peut faire mieux, en remarquant que $(n - 1)$ racines suffisent : en écrivant

$$L = K(x_1, \dots, x_{n-1})$$

on trouve

$$L : K \leq n^{n-1}.$$

Pour affiner encore la majoration, procédons « pas à pas », en ne prenant qu'une fois chaque racine. On part donc de l'ensemble $\{a_1, \dots, a_m\}$ des racines de P ; l'entier m est inférieur à n , et les a_i sont deux à deux distincts. Le corps de rupture est $L = K(a_1, a_2, \dots, a_m)$, son degré est le produit du degré de a_1 sur K , du degré de a_2 sur $K(a_1)$, du degré de a_3 sur $K(a_1, a_2)$, etc.

Or

a_1 est racine de $P \in K[X]$,

a_2 est racine de $\frac{P}{X - a_1} \in K(a_1)[X]$,

a_3 est racine de $\frac{P}{(X - a_1)(X - a_2)} \in K(a_1, a_2)[X]$, etc.

En définitive, le degré de a_{i+1} sur $K(a_1, a_2, \dots, a_i)$ est inférieur à $n - i$, d'où la majoration

$$L : K \leq n(n-1) \dots (n-m+1) \leq n!$$

On a montré :

Le degré du corps de rupture est inférieur à la factorielle du degré du polynôme.

Dans bien des cas cette majoration est encore grossière, mais on montre que c'est « globalement » la meilleure : pour tout n , il existe un corps K et un polynôme de degré n sur K dont le corps de rupture sur K est *exactement* de degré $n!$. On peut se douter qu'il s'agira du corps de rupture de l'équation générale de degré n ... (voir p. 195).

Quelques exemples.

- Si P est de degré n et possède déjà m racines dans le corps de base K , en comptant les ordres de multiplicité, il est clair qu'on majorera le degré du corps de rupture par $(n-m)!$

- Pour un polynôme de degré 2 sans racine dans K , le corps de rupture est une extension quadratique : c'est la valeur maximum $2! = 2$.

- Pour un polynôme de degré 3, le degré du corps de rupture est inférieur à $3! = 6$.

Cette valeur 6 est atteinte pour $X^3 - 2 \in \mathbb{Q}[X]$: on a vu que le corps de rupture est $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$, de degré 6.

Par contre, le même $X^3 - 2$ est toujours irréductible sur $\mathbb{Q}(j) = \mathbb{Q}(\sqrt{-3})$, mais le degré de son corps de rupture sur ce corps de base est 3.

- Pour $X^3 - 1$ sur $\mathbb{Q}$, le corps de rupture est $\mathbb{Q}(\sqrt{-3})$, extension quadratique.

- Le polynôme $X^4 - 2$ est irréductible sur $\mathbb{Q}$, son corps de rupture est $\mathbb{Q}(\sqrt[4]{2}, i)$, de degré 8 bien inférieur à la valeur maximale $4! = 24$.

- Les racines complexes de

$$1 + X^2 + X^4 \in \mathbb{Q}[X]$$

sont les racines carrées des racines complexes de $1 + X + X^2$, ce sont donc

$$j, \quad -j, \quad j^2, \quad -j^2.$$

sur à $n - i$, d'où la

factorielle du degré

mais on montre que
un corps K et un
est *exactement* de
ture de l'équation

as dans le corps de
à, il est clair qu'on
- m)!

ans K , le corps de
a valeur maximum

orps de rupture est

$[X]$: on a vu que le
6.

irréductible sur
de rupture sur ce

ce est $\mathbb{Q}(\sqrt{-3})$.

$\mathbb{Q}$, son corps de
teur à la valeur

le $1 + X + X^2$, ce

Par suite, le corps de rupture de $1 + X^2 + X^4$ sur $\mathbb{Q}$ est l'extension quadratique $\mathbb{Q}(\sqrt{-3})$. On trouve, comme degré, 2 au lieu de la majoration $4! = 24$...

- En posant $x = \sqrt[3]{1 - \sqrt{2}}$ et $y = \sqrt[3]{1 + \sqrt{2}}$ (radicaux réels) on a trouvé comme polynôme minimum commun

$$X^6 - 2X^3 - 1 \in \mathbb{Q}[X].$$

Les racines de ce polynôme sont

$$x, \quad jx, \quad j^2x, \quad y, \quad jy, \quad j^2y$$

et, comme xy est la racine cubique de -1 , on trouve $y = -\frac{1}{x}$.

Le corps de rupture du polynôme est engendré par x et j sur $\mathbb{Q}$, c'est donc $\mathbb{Q}(x, \sqrt{-3})$, il est de degré $6 \times 2 = 12$ car $\mathbb{Q}(x)$ est réel.

- Pour un polynôme pair de degré 4, soit

$$P = X^4 + aX^2 + b,$$

les racines sont $\pm \sqrt{\frac{-a \pm \sqrt{a^2 - 4b}}{2}}$, donc le corps de rupture est l'extension suivante du corps de base K

$$K\left(\sqrt{a^2 - 4b}, \sqrt{\frac{-a + \sqrt{a^2 - 4b}}{2}}, \sqrt{\frac{-a - \sqrt{a^2 - 4b}}{2}}\right).$$

Le degré est alors 1, 2, 4, ou 8.

Notons que, si P est irréductible (ce qui exige, entre autres, $\sqrt{a^2 - 4b} \notin K$), toute racine est de degré 4, donc le corps de rupture est de degré multiple de 4 : c'est 4 ou 8. Ces deux cas peuvent se produire : le corps de rupture de

$$X^4 + 1 \in \mathbb{Q}[X]$$

est $\mathbb{Q}(\sqrt{2}, i)$, de degré 4, alors que pour

$$X^4 - 2 \in \mathbb{Q}[X]$$

c'est $\mathbb{Q}(\sqrt[4]{2}, i)$, de degré 8.

Une remarque : le calcul

$$\sqrt{\frac{-a + \sqrt{a^2 - 4b}}{2}} \cdot \sqrt{\frac{-a - \sqrt{a^2 - 4b}}{2}} = \sqrt{b}$$

montre que le corps de rupture de $X^4 + aX^2 + b$ est égal à l'extension

$$K\left(\sqrt{\frac{-a + \sqrt{a^2 - 4b}}{2}}, \sqrt{b}\right)$$

qui se réduit à

$$K\left(\sqrt{\frac{-a + \sqrt{a^2 - 4b}}{2}}\right)$$

si, et seulement si, ce corps contient $\sqrt{b}$. On reviendra sur la discussion (voir p. 178).

Les corps cyclotomiques.

Les racines n -ièmes de l'unité pour un corps sont les racines de $X^n - 1$, dans le corps de rupture de ce polynôme.

On va se borner à la caractéristique nulle. On part donc de

$$X^n - 1 \in \mathbb{Q}[X]$$

et on remarque successivement :

- le dérivé de $X^n - 1$ est nX^{n-1} qui est premier avec $X^n - 1$ (pourquoi ?);
- les racines de $X^n - 1$ sont toutes simples, il y en a donc n distinctes;
- si n est impair, la seule racine réelle est 1;
- si n est pair, les seules racines réelles sont 1 et -1 , donc $X^n - 1$ est alors divisible par $X^2 - 1$;
- les $(n - 1)$ racines autres que 1 sont les racines de

$$T_n = \frac{X^n - 1}{X - 1} = 1 + X + X^2 + \dots + X^{n-1}.$$

En fait, si l'on appelle $\omega_n = e^{\frac{2i\pi}{n}}$ le nombre complexe $\cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$, alors les racines n -ièmes de l'unité forment la suite des n premières puissances de ω_n , soit

$$(1, e^{\frac{2i\pi}{n}}, e^{\frac{4i\pi}{n}}, \dots, e^{\frac{2mi\pi}{n}}, \dots, e^{\frac{2(n-1)i\pi}{n}}).$$

Ce sont les sommets d'un polygone régulier de n côtés inscrit dans le cercle unité.

Le corps engendré sur $\mathbb{Q}$ par ces racines est le corps de rupture de $X^n - 1$ sur $\mathbb{Q}$; il suffit bien sûr de ω_n pour l'engendrer.

Autrement dit, si l'on appelle **corps cyclotomique** d'indice n le corps de rupture de $X^n - 1$ sur $\mathbb{Q}$, c'est une extension simple de $\mathbb{Q}$, égale à $\mathbb{Q}(\omega_n)$: c'est le corps engendré par les racines n -ièmes de l'unité.

Un exercice classique et simple montre que, si l'on part non de ω_n mais d'une puissance $(\omega_n)^m$, on obtiendra *toutes* les autres comme puissances de celle-ci si, et seulement si, m est premier avec n ; un tel $(\omega_n)^m$ est élément primitif du corps cyclotomique d'indice n , on l'appelle naturellement une **racine primitive** de l'unité. Le nombre de ces racines primitives est $\varphi(n)$, nombre d'entiers inférieurs à n premiers avec n .

Le deg
sur $\mathbb{Q}$ de

Si n est
minimum
algébrique
Dans le
primitive
parcourt
qui signifie
dans $\mathbb{Q}$),
polynôme
l'extension
s'appelle

- Les racines quatrièmes sont $1, i, -1, -i$, seules i et $-i$ sont primitives.

- Pour $n = 6$, il n'y a encore que deux racines primitives,

$$e^{\frac{2i\pi}{6}} = -j^2 \quad \text{et} \quad e^{\frac{10i\pi}{6}} = -j.$$

- Si n est premier, toutes les racines autres que 1 sont primitives, ce sont les racines de

$$T_n = 1 + X + \cdots + X^{n-1}.$$

- Si n est primaire, c'est-à-dire puissance d'un nombre premier, soit $n = p^s$, les racines primitives sont les $e^{\frac{2ik\pi}{n}}$ où k est inférieur à n et non multiple de p . Il y a p^{s-1} multiples de p inférieurs à n , donc $p^s - p^{s-1} = n \left(1 - \frac{1}{p}\right)$ racines primitives n -ièmes de l'unité.

Le degré du corps cyclotomique d'indice n dépendra du polynôme irréductible sur $\mathbb{Q}$ dont sera racine $\omega_n = e^{\frac{2i\pi}{n}}$. Ce polynôme sera un diviseur de

$$T_n = 1 + X + X^2 + \cdots + X^{n-1}.$$

Si n est premier, on montre que T_n est irréductible, c'est donc le polynôme minimum de ω_n et le degré de l'extension cyclotomique est $(n-1)$. (Voir *Le Défi algébrique*, tome II, page 336).

Dans le cas général, il se trouve que le polynôme ayant pour racines les racines primitives n -ièmes de l'unité, c'est-à-dire le produit des $X - (\omega_n)^m$ quand m parcourt les $\varphi(n)$ entiers inférieurs à n premiers avec n , est à coefficients dans $\mathbb{Q}$ (ce qui signifie que les fonctions symétriques élémentaires des racines primitives sont dans $\mathbb{Q}$). Il y a mieux : le polynôme est alors irréductible sur $\mathbb{Q}$, c'est donc le polynôme minimum commun des racines primitives n -ièmes, et le degré de l'extension est alors $\varphi(n)$. (Voir *Le Défi algébrique*, tome II, p. 334). Ce polynôme s'appelle **polynôme cyclotomique** d'indice n , et se note Φ_n .

- On aura ainsi :

$$\Phi_1 = -1 + X$$

$$\Phi_2 = 1 + X$$

$$\Phi_3 = 1 + X + X^2$$

$$\Phi_4 = 1 + X^2$$

$$\Phi_5 = 1 + X + X^2 + X^3 + X^4$$

$$\Phi_6 = 1 - X + X^2$$

$$\Phi_7 = 1 + X + X^2 + X^3 + X^4 + X^5 + X^6.$$

- Pour $n = 8$, on calcule $\varphi(8) = 4$, les racines primitives huitièmes étant

$$e^{\frac{2i\pi}{8}}, \quad e^{\frac{6i\pi}{8}}, \quad e^{\frac{10i\pi}{8}}, \quad e^{\frac{14i\pi}{8}},$$

c'est-à-dire respectivement

$$\frac{1+i}{\sqrt{2}}, \quad \frac{-1+i}{\sqrt{2}}, \quad \frac{-1-i}{\sqrt{2}}, \quad \frac{1-i}{\sqrt{2}}.$$

Ce sont les quatre racines du polynôme $\Phi_8 = X^4 + 1$ qui est donc leur polynôme minimum commun sur $\mathbb{Q}$.

- Une racine primitive neuvième est une racine cubique de j , de polynôme minimum

$$\Phi_9 = 1 + X^3 + X^6.$$

A l'indice 10, le polynôme minimum de $e^{\frac{2in}{10}}$ est de degré $\varphi(10) = 4$, on trouve

$$\Phi_{10} = 1 - X + X^2 - X^3 + X^4$$

car l'opposé d'une racine primitive cinquième est racine primitive dixième.

Puis c'est

$$\Phi_{11} = \sum_{i=0}^{10} X^i.$$

A l'indice 12, une racine primitive est ij , de polynôme minimum

$$\Phi_{12} = 1 - X^2 + X^4.$$

- Pour p premier, c'est toujours

$$\Phi_p = \sum_{i=0}^{p-1} X^i.$$

Le corps de rupture d'une équation binôme.

Le problème de départ de toute cette théorie était celui de l'expression des racines d'un polynôme à partir des coefficients en ne faisant intervenir que des opérations rationnelles et des extractions de radicaux. Tout revient, on l'avait signalé, à ramener la résolution à celle d'une suite d'équations binômes, c'est-à-dire de la forme

$$X^n - \alpha = 0$$

où α est dans le corps de base.

D'où l'importance des corps de rupture de ces équations, dont on a vu déjà des exemples. Or il est évident que l'on obtient toutes les racines du polynôme

$$X^n - \alpha \in K[X]$$

en multipliant l'une d'elles par toutes les racines n -ièmes de l'unité (tout cela dans une extension adéquate de K , par exemple $\mathbb{C}$ si K est un sous-corps de $\mathbb{C}$).

En d'autres termes, le corps de rupture est $K(\omega_n, \beta)$, où β est une racine n -ième de α dans K et ω_n est $e^{\frac{2in}{n}}$ (ou toute racine primitive n -ième de l'unité sur K) : c'est une extension par radicaux successifs, qui est aussi extension du corps cyclotomique d'indice n sur K .

On a signalé les dangers de l'écriture $\sqrt[n]{\alpha}$ pour β tant que l'on n'a pas

QUELQUE

adjoint ω_n ,
alors sur le

Il est com
 n , c'est-à-di
mais arbitra
élément pri
de K .

C'est pou
nécessaires (
dès le départ
sur K est er
irréductible

Les équation

L'importa
d'irréductibi
toute équati

$$X^n - \alpha$$

La réciproqu

Pour y vo
racine n -ième
La factorisat

Supposons X
 $K[X]$, donc
produit de q
constant est

où les s_i form
On calcule

et cet élément
Si l'on élève

puisque ω est

$= X^4 + 1$ qui est $\mathbb{Q}$.

ne cubique de j , de

$\frac{2in}{e^{10}}$ est de degré

X^4

est racine primitive

polynôme minimum

de l'expression des
et intervenir que des
et revient, on l'avait
ons binômes, c'est-à-

dont on a vu déjà des
nes du polynôme

l'unité (tout cela dans
sous-corps de $\mathbb{C}$).

est une racine n -ième
de l'unité sur K) : c'est
extension du corps

ant que l'on n'a pas

adjoind ω_n , donc les racines n -ièmes de l'unité : le choix de la racine n -ième influe alors sur le corps obtenu.

Il est commode de supposer que K contient déjà le corps cyclotomique d'indice n , c'est-à-dire les racines n -ièmes de l'unité. On peut alors noter $\sqrt[n]{\alpha}$ l'une, fixée mais arbitraire, des racines n -ièmes de α dans le corps de rupture, et c'est un élément primitif de ce corps de rupture qui est ainsi une extension par radical de K .

C'est pourquoi on adjoindra souvent dès le départ les racines de l'unité nécessaires (c'est ce que l'on a fait pour l'équation générale de degré 3, où l'on a dès le départ adjoind j). Le degré du corps de rupture $K(\sqrt[n]{\alpha})$ de $X^n - \alpha \in K[X]$ sur K est en ce cas inférieur à n , il est égal à n si, et seulement si, $X^n - \alpha$ est irréductible sur K .

Les équations binômes de degré premier.

L'importance des équations binômes mérite que l'on cherche des critères d'irréductibilité. Une condition nécessaire est évidente, pour tout corps K et toute équation binôme $X^n - \alpha \in K[X]$:

$X^n - \alpha$ irréductible sur $K \Rightarrow \alpha$ n'a pas de racine n -ième dans K .

La réciproque est fautive en général.

Ainsi, -4 n'a pas de racine quatrième dans $\mathbb{Q}$, mais l'égalité

$$(X^2 - 2X + 2)(X^2 + 2X + 2) = X^4 + 4$$

montre que $X^4 + 4$ est quand même réductible sur $\mathbb{Q}$.

Pour y voir de plus près, introduisons une racine n -ième de α , soit β , et une racine n -ième primitive de 1, soit ω (tout cela dans une extension adéquate de K). La factorisation totale de $X^n - \alpha$ dans le corps $K(\omega, \beta)$ s'écrit

$$X^n - \alpha = (X - \beta)(X - \omega\beta) \dots (X - \omega^{n-1}\beta).$$

Supposons $X^n - \alpha$ réductible sur K et appelons T un de ses facteurs propres dans $K[X]$, donc de degré q entre 1 et $n - 1$. Ce polynôme $T \in K[X]$ doit être un produit de q facteurs de degré 1 de la décomposition ci-dessus, son terme constant est donc

$$T(0) = (-\omega^{s_1}\beta)(-\omega^{s_2}\beta) \dots (-\omega^{s_q}\beta)$$

où les s_i forment une suite strictement croissante de q entiers entre 1 et $(n - 1)$. On calcule

$$T(0) = (-1)^q \beta^q \omega^{s_1 + s_2 + \dots + s_q}$$

et cet élément est dans K car T est un facteur de $X^n - \alpha$ dans $K[X]$.

Si l'on élève à la puissance n , il reste

$$(T(0))^n = (-1)^{nq} \alpha^q$$

puisque ω est racine n -ième de 1 et β est racine n -ième de α .

On pourra aller plus loin — c'est-à-dire montrer que α possède une racine n -ième dans K — si n et q sont premiers entre eux. Et cette condition est automatiquement réalisée si n est premier.

On supposera donc désormais n premier, et on écrira bien sûr une identité de Bezout entre n et q qui sont premiers entre eux (car q est entre 1 et $n - 1$) : il existe u et v entiers avec $un + vq = 1$, d'où

$$\alpha = \alpha^{un+vq} = (-1)^{nqv}(T(0))^{nv}\alpha^{nu}.$$

Il suffit alors de poser

$$\beta = (-1)^{nv}\alpha^u(T(0))^v.$$

C'est un élément du corps K et sa puissance n -ième est égale à α .

En conclusion : pour n premier, on a montré

$X^n - \alpha$ réductible sur $K \Rightarrow \alpha$ possède une racine n -ième dans K .

C'est la réciproque de l'implication évidente du début.

On énoncera donc :

Pour p premier, les corps sur lesquels le polynôme $X^p - \alpha$ est réductible sont ceux qui possèdent une racine p -ième de α .

Quelques remarques (p est toujours un nombre premier) :

- si K contient une racine p -ième de l'unité autre que 1 (donc toutes), alors une équation binôme de degré p est irréductible ou totalement factorisable sur K ;
- si α n'a pas de racine p -ième dans K , le degré sur K de toutes racine p -ième de α est p , son polynôme minimum étant $X^p - \alpha$;
- si α n'a pas de racine m -ième dans K (m est ici arbitraire, pas premier), tout facteur propre de $X^m - \alpha$ dans $K[X]$ est de degré non premier avec m ; il suffit de regarder attentivement le raisonnement ci-dessus.

Exercices.

1. Montrer qu'en caractéristique 2 il existe des équations de degré 2 n'ayant de racine dans aucune extension de la forme $K(\sqrt{x})$.
2. Chercher toutes les extensions quadratiques de $\mathbb{Z}/3$.
3. Des polynômes irréductibles différents peuvent avoir des corps de rupture égaux. Donner des exemples sur $\mathbb{Q}$.
4. Quel est le degré sur $\mathbb{Q}$ du corps de rupture de $1 + X^3 + X^9$? de $X^5 - 1$? de $X^8 - 2$?
5. Étudier le corps de rupture de $1 + X + X^3$ sur $\mathbb{Q}$, puis sur $\mathbb{Z}/2$. Dans ce dernier cas, on montrera que le polynôme est irréductible, et que, si α est une racine dans une extension, les autres sont α^2 et $\alpha + \alpha^2$, d'où l'on conclura que le corps de rupture est de degré 3.

QUELQUES

6. Montre
nulle si

7. La consi

0 et 1 se

Si p est

doit être

entier q

En dedu

premier,

On mon

oui pour

8. Une exte
l'unité ?

9. Sur un c
d'élémén

Montrer
avec n vé

Que se p

10. Étudier l

11. Pour n ir

12. Sur un co
toujours

modulo 1

13. Toute rac
 m de n . E

La vérifie

Prouver

ossède une racine
ette condition est

ûr une identité de
tre 1 et $n - 1$) : il

e à α .

e dans K .

ynôme $X^p - \alpha$ est
 p -ième de α .

ic toutes), alors une
factorisable sur K ;
outes racine p -ième

, pas premier), tout
r avec m : il suffit de

é $\mathbb{Q}$ n'ayant de racine

ps de rupture égaux.

X^9 ? de $X^5 - 1$? de

2. Dans ce dernier cas,
t une racine dans une
ue le corps de rupture

6. Montrer que la somme des puissances q -ièmes des racines n -ièmes de l'unité est nulle si q n'est pas multiple de n , égale à n si q est multiple de n .

7. La construction à la règle et au compas d'un polygone régulier de p côtés à partir de 0 et 1 se ramène à la constructibilité du nombre $e^{\frac{2i\pi}{p}}$.
Si p est premier, on montrera que ce nombre est de degré $p - 1$, donc que $p - 1$ doit être une puissance de 2, soit $p = 1 + 2^r$. On vérifiera ensuite que, si r est un entier qui possède un diviseur impair, alors $1 + 2^r$ n'est pas premier.

En déduire que, pour qu'un polygone régulier de p côtés soit constructible, p étant premier, il est nécessaire que p soit de la forme

$$p = 1 + 2^{2^m}.$$

On montre que c'est suffisant. Mais $1 + 2^{2^m}$ est-il toujours premier ? La réponse est oui pour $m = 1, 2, 3, 4$, non pour $m = 5$.

8. Une extension de degré fini sur $\mathbb{Q}$ peut-elle contenir une infinité de racines de l'unité ?

9. Sur un corps K contenant les racines n -ièmes de l'unité, chercher des exemples d'éléments a et b différents tels que $X^n - a$ et $X^n - b$ aient même corps de rupture.

Montrer que la condition nécessaire et suffisante est : il existe un entier m premier avec n vérifiant

$$\sqrt[n]{a^m b^{-1}} \in K.$$

Que se passe-t-il si l'on supprime l'hypothèse sur K (par exemple $K = \mathbb{Q}$) ?

10. Étudier le corps cyclotomique d'indice 12.

11. Pour n impair, les corps cyclotomiques d'indices n et $2n$ sont égaux.

12. Sur un corps de caractéristique non nulle, les polynômes cyclotomiques ne sont pas toujours irréductibles. On vérifiera l'égalité

$$\Phi_{12} = (X^2 - 5X + 1)(X^2 + 5X + 1)$$

modulo 11.

13. Toute racine n -ième de l'unité est racine primitive m -ième pour un unique diviseur m de n . En déduire l'égalité

$$X^n - 1 = \prod_{m|n} \Phi_m.$$

La vérifier pour $n = 6, 8, 10, 12$.

Prouver que les coefficients de tous les Φ_n sont des entiers.

Groupe de Galois d'un polynôme

A plusieurs reprises on a trouvé commode d'associer à un polynôme donné certaines permutations de la famille de ses racines ; c'est ainsi, en particulier, que l'on a résolu les équations de degrés 3 et 4.

Ceci dit, dans le cas des équations *générales*, celles dont les coefficients sont des indéterminées, il n'y a aucune raison de privilégier certaines permutations plutôt que d'autres. Il n'en va pas de même pour un polynôme « concret » : ainsi, les racines du polynôme

$$(X^2 - 3)(X^2 - 2) = X^4 - 5X^2 + 6 \in \mathbb{Q}[X]$$

forment la famille $(\sqrt{3}, -\sqrt{3}, \sqrt{2}, -\sqrt{2})$ et il est intuitif que, vis-à-vis de ce polynôme, la permutation échangeant $\sqrt{3}$ et $-\sqrt{3}$ est plus « naturelle » que celle qui échange $\sqrt{3}$ et $\sqrt{2}$.

C'est cette classification des permutations entre « bonnes » et « mauvaises » qui va nous occuper maintenant.

Bien entendu, en parlant des racines, on se place toujours dans le corps de rupture du polynôme, ou tout corps plus grand (par exemple un corps algébriquement clos contenant tous les coefficients). Il suffira de prendre $\mathbb{C}$ si les coefficients sont des nombres, réels ou complexes.

Quelques rappels sur les groupes.

On signale ici « en vrac » quelques notions de théorie des groupes dont on se servira parfois dans la suite. Mais on pourra s'en passer pour la majeure partie de l'exposé.

On notera par juxtaposition la loi de composition dans le groupe G . Alors :

- l'ordre de G est son nombre d'éléments ;
- le sous-groupe engendré par une partie T de G est formé de tous les composés de familles finies d'éléments de T ou de leurs inverses ;
- un groupe engendré par un élément, donc formé des puissances de cet élément, est dit **cyclique** ;
- l'ordre d'un élément $x \in G$ est l'ordre du sous-groupe qu'il engendre, c'est aussi, quand il existe de tels entiers, le plus petit entier $n \geq 1$ vérifiant $x^n = 1$; on

dit alors que x est d'ordre fini (c'est le cas forcément si G est fini) et l'on montre (par division euclidienne) :

$$x^m = 1 \Leftrightarrow n \text{ divise } m;$$

- l'ordre de tout sous-groupe (donc aussi de tout élément) divise l'ordre du groupe et le quotient s'appelle l'**indice** du sous-groupe ;
- pour tout $n \in \mathbb{N}$, les groupes cycliques d'ordre n sont tous isomorphes au groupe additif $\mathbb{Z}/n$ des classes d'entiers modulo n ; on notera C_n le groupe cyclique d'ordre n et, pour n premier, c'est le seul groupe d'ordre n ;
- les classes modulo n d'entiers premiers avec n forment un groupe multiplicatif, noté $(\mathbb{Z}/n)^*$; si p est premier, c'est le groupe multiplicatif $\mathbb{Z}/p \setminus 0$ et il est cyclique ;
- jusqu'à l'ordre 5, tous les groupes sont abéliens : ce sont

$$\text{id}, C_2, C_3, C_2 \times C_2, C_4, C_5;$$

- un élément $a \in G$ définit la transformation

$$x \rightarrow axa^{-1}$$

du groupe qui est un automorphisme (bijection conservant la loi) appelé **conjugaison** par a ou automorphisme intérieur ; deux éléments se correspondant par une conjugaison sont dits conjugués ;

- un sous-groupe H invariant par toutes les conjugaisons est dit **normal** dans G et l'on note alors

$$H \triangleleft G;$$

- le noyau de tout homomorphisme défini sur G est un sous-groupe normal et, inversement, tout sous-groupe normal H de G est noyau de la surjection canonique de G sur le **groupe quotient** G/H ou groupe des classes de G modulo H (c'est-à-dire modulo la relation d'équivalence $xy^{-1} \in H$) ;

- l'image d'un homomorphisme ϕ défini sur G est isomorphe au groupe quotient $G/\text{Ker } \phi$, où $\text{Ker } \phi$ est le noyau de ϕ .

Les groupes symétriques.

Les exemples essentiels de groupes sont les groupes de permutations, dont les éléments sont des bijections d'un ensemble donné sur lui-même.

Si l'ensemble est fini, on le note $\{1, 2, \dots, n\}$, et une permutation est une suite $(i_1, \dots, i_n)$, où les i_j sont des entiers deux à deux distincts compris entre 1 et n . Le complémentaire de l'ensemble des points fixes s'appelle le support de la permutation, et une permutation est dite **cyclique** si elle est formée de la suite des transformés successifs d'un de ses éléments : on la notera alors souvent par cette suite elle-même, et on dit que c'est un **cycle**.

Ainsi, la permutation $(4 \ 1 \ 3 \ 2 \ 5)$ de 5 éléments est un cycle, et s'écrit $(1 \ 4 \ 2)$ ou $(4 \ 2 \ 1)$ ou $(2 \ 1 \ 4)$ en « notation cyclique ». Réciproquement, le cycle $(2 \ 4 \ 3 \ 5)$ s'écrira $(1 \ 4 \ 5 \ 3 \ 2)$ en « notation usuelle ».

On u

On r
permut

• l'or
• la l
ordre; t
l'échang

• deu
• tou
disjoints

• l'or
cyclique;

• tou
décompe
parler de
- 1);

• la si
• les p
d'indice :

• le gr
• le gr

{id, (1, 2)
groupe a
d'ordre 6

• dans
normal, i

• pour
pas d'aut

Les group

Qu'y a-
quatrième
racines, re
peu de va

La ques
bien avan
rationnell
 σ telles qu

soit égal à

Mais à l
valeurs qu

et l'on montre

l'ordre du

somorphes au

C_n le groupe

de n ;

est un groupe

additif $\mathbb{Z}/p\mathbb{Z}$ et il

la loi) appelé
correspondant

est normal dans

groupe normal et,
la surjection
de G modulo H

est au groupe

ations, dont les

est une suite

entre 1 et n . Le

support de la

de la suite des

uvent par cette

est un cycle, et
tion cyclique ».

(1 4 5 3 2) en

On utilisera en général la notation cyclique.

On note Σ_n le **groupe symétrique** de degré n , ou groupe de toutes les permutations de n éléments. On montre alors :

- l'ordre de Σ_n est $n!$;
- la **longueur** d'un cycle, ou nombre d'éléments de son support, est égale à son ordre; un cycle de longueur 2 s'appelle une **transposition**, et consiste donc en l'échange de deux éléments;
- deux cycles disjoints, c'est-à-dire à supports disjoints, commutent;
- toute permutation est, de manière unique, produit de cycles deux à deux disjoints, que l'on appelle ses **composantes** cycliques;
- l'ordre d'une permutation est le P.P.C.M. des longueurs de ses composantes cycliques;
- toute permutation est produit de transpositions; il y a plusieurs décompositions mais la parité du nombre de facteurs est constante, et permet de parler de permutations **paires** (ou de signature $+1$) et **impaires** (ou de signature -1);
- la signature d'un produit est le produit des signatures;
- les permutations paires de Σ_n forment le **groupe alterné** A_n , seul sous-groupe d'indice 2 dans Σ_n ;
- le groupe Σ_2 est cyclique, égal à C_2 ;
- le groupe Σ_3 est non abélien, ses sous-groupes autres que id et lui-même sont $\{\text{id}, (1\ 2)\}$, $\{\text{id}, (2\ 3)\}$, $\{\text{id}, (1\ 3)\}$, et $\{\text{id}, (1\ 2\ 3), (1\ 3\ 2)\}$, ce dernier étant le groupe alterné A_3 , cyclique, et seul normal parmi les quatre; les seuls groupes d'ordre 6 sont Σ_3 et C_6 ;
- dans le groupe Σ_4 il y a, outre id , A_4 , et Σ_4 lui-même, un seul sous-groupe normal, il est d'ordre 4 et formé de

$$\text{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3);$$

- pour $n \geq 5$, A_n n'a aucun sous-groupe propre normal autre que id , et Σ_n n'a pas d'autre sous-groupe propre normal que id et A_n .

Les groupes et les équations : un exemple historique.

Qu'y a-t-il de commun entre les résolutions des équations du troisième et du quatrième degré ? Dans les deux cas, on a utilisé une « fonction auxiliaire » des racines, respectivement $(x_1 + jx_2 + j^2x_3)^3$ et $x_1x_2 + x_3x_4$, qui ne prenait que peu de valeurs distinctes quand on effectuait les 6 ou 24 permutations.

La question a été étudiée dans sa généralité pour un degré n arbitraire, et ceci bien avant Galois. On la posait de la manière suivante : on part d'une fonction rationnelle de n indéterminées, soit $T(X_1, \dots, X_n)$, et on étudie les permutations σ telles que

$$T(X_{\sigma(1)}, \dots, X_{\sigma(n)})$$

soit égal à $T(X_1, \dots, X_n)$. Elles forment un sous-groupe, soit H , de Σ_n .

Mais à l'époque, on n'employait pas ce langage : on parlait du « nombre de valeurs que peut prendre la fonction T quand on y permute les valeurs X_i ». Ce

nombre de valeurs est le cardinal de l'image de Σ_n par l'application

$$\sigma \rightarrow T(X_{\sigma(1)} \dots, X_{\sigma(n)}).$$

Les permutations σ_1 et σ_2 donneront la même valeur si, et seulement si, $\sigma_1 \sigma_2^{-1}$ est dans H (on dit que σ_1 et σ_2 sont égales modulo H à gauche). Dans ces conditions, pour tout $s \in \Sigma_n$, le nombre de $\sigma \in \Sigma_n$ donnant même valeur sera égal au cardinal de H . En d'autres termes, le « nombre de valeurs de la fonction T » est égal à l'indice de H , c'est un diviseur de l'ordre $n!$ de Σ_n .

C'est Lagrange qui a amorcé la théorie de ce point de vue et ses idées ont été approfondies par Cauchy avant Galois, sans le langage actuel de théorie des groupes, mais facile à « traduire ». On cherchera dès lors, comme pour $n = 3$ et $n = 4$, une fonction rationnelle des racines qui, quand on effectue toutes les permutations, ne prend un nombre différent de valeurs ni trop grand ni trop petit : pas trop grand, car on veut que la fonction satisfasse une équation de degré inférieur à celle donnée, et pas trop petit pour qu'elle permette de « récupérer » les racines. Car si m est ce nombre de valeurs, notre fonction est racine d'une équation de degré m sur le corps de base.

A partir de $n = 5$, Cauchy a montré que « ça ne marchait plus ». Un des énoncés de son résultat est le suivant : « Si $p \geq 3$ est un diviseur premier de n et si une fonction de n lettres prend moins de $(p - 1)$ valeurs distinctes, alors elle ne peut en prendre plus de deux ».

Traduction en termes de groupes : si H est un sous-groupe de Σ_n d'indice inférieur à $(p - 1)$, alors il est d'indice 1 ou 2, donc égal à Σ_n ou à A_n . Autrement dit

$$\Sigma_n : H < p \Rightarrow H \supset A_n.$$

Une conséquence : si n est premier, toute « fonction intermédiaire » construite à partir des racines de l'équation générale est, soit racine d'une équation irréductible de degré supérieur à n (et on n'est pas avancé), soit racine d'une équation de degré 1 ou 2 (et elle ne sert pas à grand-chose...).

La démonstration « moderne » utilise la théorie des groupes. On part d'un cycle γ de longueur p . Alors les sous-ensembles $H, \gamma H, \gamma^2 H, \dots, \gamma^{p-1} H$ ne peuvent être deux à deux disjoints, car p fois l'ordre de H est strictement supérieur à l'ordre de Σ_n . On prend donc $i \neq j$ avec $\gamma^i H \cap \gamma^j H \neq \emptyset$, d'où l'on tire $\gamma^{i-j} \in H$. Mais le sous-groupe engendré par γ^{i-j} est contenu dans celui, d'ordre premier, engendré par γ , il lui est donc égal, d'où l'on déduit $\gamma \in H$. Dès lors, si H contient tous les cycles de longueur p , il contient tous ceux de longueur 3, d'après le calcul :

$$(1 \ 2 \ 3 \ \dots \ p)(p \ (p-1) \ \dots \ 4 \ 2 \ 3 \ 1) = (2 \ 4 \ 3).$$

Or le groupe alterné A_n est engendré par les cycles de longueur 3, ce qui prouve bien la conclusion.

Un exemple de fonction qui « ne prend que deux valeurs » est

$$d = \prod_{i < j} (X_i - X_j)$$

alors que celles qui « ne prennent qu'une valeur » sont les symétriques.

Dès lors, on
valeurs, soit T
 $T = A + Bd$.

Si l'on remp

les fonctions s
discriminant d
degré n de P es
l'équation gén
de degré supér

Dès lors, on vérifie que d^2 est symétrique, et que, si T ne prend que deux valeurs, soit T et T_1 , alors $T + T_1$ et $Td - T_1d$ sont symétriques, d'où l'écriture $T = A + Bd$ avec A et B symétriques.

Si l'on remplace les X_i par les racines de

$$P \in K[X],$$

les fonctions symétriques sont des éléments de K , le carré $d^2 = \Delta$ s'appelle le discriminant de P , il est dans K . Le résultat de Cauchy montre que, au moins si le degré n de P est premier et si l'on construit une fonction rationnelle des racines de l'équation générale de degré n , alors, ou bien elle est racine d'une équation de degré supérieur à n sur K ou bien elle est dans l'extension quadratique $K(\sqrt{\Delta})$.

t si, $\sigma_1 \sigma_2^{-1}$
Dans ces
r sera égal
ion T » est

ées ont été
héorie des
ir $n = 3$ et
toutes les
nd ni trop
quation de
rmette de
onction est

». Un des
er de n et si
lors elle ne

Σ_n d'indice
Autrement

construite
équation
eine d'une

part d'un
 $\gamma^{p-1}H$ ne
trictement
d'où l'on
dans celui,
 $\gamma \in H$. Dès
s ceux de

qui prouve

ques.

Bonnes et mauvaises permutations des racines

• Partons d'un polynôme de degré 2 sur $\mathbb{Q}$, soit $X^2 + aX + b$, et supposons ses racines x et y distinctes. On a vu que deux cas se présentent :

- si $a^2 - 4b$ possède une racine carrée dans $\mathbb{Q}$, alors x et y sont dans $\mathbb{Q}$ et le seul automorphisme du corps $\mathbb{Q}$ est la transformation identique : la transposition de x et y ne correspond pas à un automorphisme du corps de rupture, ce sera une « mauvaise » permutation ;
- par contre, si $a^2 - 4b$ n'est pas un carré dans $\mathbb{Q}$, le corps de rupture est l'extension quadratique $\mathbb{Q}(\sqrt{a^2 - 4b})$, dont tout élément s'écrit de manière unique $u + vd$, où u et v sont rationnels, d étant une racine carrée de $a^2 - 4b$. Or la transformation

$$u + vd \rightarrow u - vd$$

est, comme on le vérifie facilement, un automorphisme du corps $\mathbb{Q}(d)$ et cet automorphisme échange x et y : dans ce cas la transposition des deux racines est une « bonne » permutation, car elle correspond à un automorphisme du corps de rupture.

• Prenons maintenant le polynôme

$$(X^2 - 2)(X^2 - 3) = X^4 - 5X^2 + 6 \in \mathbb{Q}[X]$$

et écrivons ses racines dans l'ordre suivant :

$$(\sqrt{2}; \quad -\sqrt{2}; \quad \sqrt{3}; \quad -\sqrt{3}).$$

Le corps de rupture est $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, égal aussi, on l'a vu, à $\mathbb{Q}(\sqrt{2} + \sqrt{3})$, et chacun de ses éléments s'écrit de manière unique

$$\alpha + \beta\sqrt{2} + \gamma\sqrt{3} + \delta\sqrt{6}$$

les coefficients étant dans $\mathbb{Q}$.

La transposition $(1 \ 2)$ échange $\sqrt{2}$ et $-\sqrt{2}$ et laisse fixe $\sqrt{3}$ et $-\sqrt{3}$, donc définit sur le corps de rupture la transformation :

$$\alpha + \beta\sqrt{2} + \gamma\sqrt{3} + \delta\sqrt{6} \rightarrow \alpha - \beta\sqrt{2} + \gamma\sqrt{3} - \delta\sqrt{6}.$$

Permutations

Appelons {
rappelons-le,
Le corps de
s'écrit $\mathbb{Q}(a_1, \dots$

Prenons u
transformatio

de $K(a_1, \dots,$
pourra s'écrire

pour plusieurs

On peut vérifier directement que c'est là un automorphisme du corps $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, on peut aussi se ramener au cas ci-dessus en considérant le corps comme une extension quadratique de $\mathbb{Q}(\sqrt{3})$, c'est-à-dire $\mathbb{Q}(\sqrt{3})(\sqrt{2})$: la transformation ci-dessus est alors l'automorphisme

$$u + v\sqrt{2} \rightarrow u - v\sqrt{2}$$

u et v étant dans $\mathbb{Q}(\sqrt{3})$.

Passons à la transposition (1 3), qui échange $\sqrt{2}$ et $\sqrt{3}$ et laisse fixe $-\sqrt{2}$ et $-\sqrt{3}$. Elle ne définit pas un automorphisme de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, car dans un tel automorphisme on ne peut avoir à la fois $\sqrt{3}$ pour image de $\sqrt{2}$ et $-\sqrt{2}$ pour image de $-\sqrt{3}$: l'image de l'opposé doit être l'opposée de l'image.

On dira que (1 2) est une bonne permutation des racines de $X^4 - 5X^2 + 6$, alors que (1 3) est une mauvaise (les racines ayant été classées dans l'ordre du début). Une autre manière de dire est la suivante : si l'on écrit (x_1, x_2, x_3, x_4) la suite des racines, la transposition (1 3) ne respecte pas la relation rationnelle $x_1 + x_2 = 0$, car l'image de $x_1 + x_2$ est $x_3 + x_2$ qui n'est pas nul.

Permutations respectant les relations.

Appelons $\{a_1, \dots, a_m\}$ l'ensemble des racines de $P \in K[X]$, ce qui signifie, rappelons-le, que l'on ne compte qu'une fois chaque racine, même multiple.

Le corps de rupture de P sur K est l'extension $K(a_1, \dots, a_m)$ dont tout élément s'écrit $Q(a_1, \dots, a_m)$ où Q est un polynôme à m indéterminées sur K .

Prenons une permutation σ des m indices. Peut-on considérer la transformation

$$Q(a_1, \dots, a_m) \rightarrow Q(a_{\sigma(1)}, \dots, a_{\sigma(m)})$$

de $K(a_1, \dots, a_m)$? La réponse est non, car un même élément de $K(a_1, \dots, a_m)$ pourra s'écrire

$$Q(a_1, \dots, a_m)$$

pour plusieurs polynômes Q et rien ne prouve que l'image soit la même.

Ainsi, les racines de

$$P = (X^2 - 2)(X^2 - 3) \in \mathbb{Q}[X]$$

sont $\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$. Avec cette numérotation, on écrit

$$1 = a_3^2 - a_1^2 \quad \text{et} \quad 1 = a_4^2 - a_2^2.$$

Permutations des racines

$X^2 + aX + b$, et que deux cas se

2, alors x et y sont dans le corps $\mathbb{Q}$ est la de x et y ne de rupture, ce sera

ins $\mathbb{Q}$, le corps de $-4b$, dont tout où u et v sont $a^2 - 4b$. Or la

phisme du corps : dans ce cas la ne » permutation, corps de rupture.

$\in \mathbb{Q}[X]$

3).

ussi, on l'a vu, à s'écrit de manière

et laisse fixe $\sqrt{3}$ et a transformation : $+ \gamma\sqrt{3} - \delta\sqrt{6}$.

Si l'on effectue la transposition de a_1 et a_3 , on trouverait pour image de 1

$$a_1^2 - a_3^2 = -1 \quad \text{et} \quad a_4^2 - a_2^2 = 1$$

ce qui est absurde.

Pour y voir plus clair, rappelons que $K(a_1, \dots, a_m)$ est quotient de l'anneau de polynômes $K[X_1, \dots, X_m]$ par l'idéal des polynômes nuls en $(a_1, \dots, a_m)$. Il est alors plus sûr de partir de l'homomorphisme surjectif d'anneaux :

$$\begin{aligned} T &\rightarrow T(a_{\sigma(1)}, \dots, a_{\sigma(m)}) \\ K[X_1, \dots, X_m] &\rightarrow K(a_1, \dots, a_m). \end{aligned}$$

Cet homomorphisme « passera, au quotient » si, et seulement si, tout polynôme nul en $(a_1, \dots, a_m)$ est aussi nul en $(a_{\sigma(1)}, \dots, a_{\sigma(m)})$.

Or une égalité $R(a_1, \dots, a_m) = 0$ avec R non nul dans $K[X_1, \dots, X_m]$ s'appelle une **relation rationnelle** (ou algébrique) entre les a_i . Les « bonnes » permutations σ seront celles qui vérifieront

$$R(a_1, \dots, a_m) = 0 \Rightarrow R(a_{\sigma(1)}, \dots, a_{\sigma(m)}) = 0$$

c'est-à-dire qui respecteront *toutes* les relations rationnelles entre les racines. Il est clair qu'elles forment un sous-groupe du groupe symétrique Σ_m .

- Si une racine est dans le corps K lui-même, toute bonne permutation devra la laisser fixe.
- Pour le polynôme

$$(X - 1)(X^2 + 1) \in \mathbb{Q}[X]$$

les deux seules bonnes permutations des trois racines sont :

$$\begin{aligned} (1, i, -i) &\rightarrow (1, i, -i) \\ (1, i, -i) &\rightarrow (1, -i, i). \end{aligned}$$

Le groupe de Galois d'un polynôme.

Reprenons notre polynôme $P \in K[X]$, de racines $a_1, \dots, a_m$. Les « bonnes » permutations des racines définissent une transformation du corps de rupture. Soit $\bar{\sigma}$ la transformation associée à la permutation σ . Alors

- $\bar{\sigma}$ est un endomorphisme du corps de rupture de P car il s'obtient par passage au quotient d'un homomorphisme d'anneaux ;
- $\bar{\sigma}$ laisse fixe les éléments de K ;
- $\bar{\sigma}$ est un *automorphisme* du corps de rupture de P , car σ^{-1} est aussi une « bonne » permutation et l'endomorphisme $\bar{\sigma}^{-1}$ qui lui correspond est inverse de $\bar{\sigma}$;
- on peut identifier σ et $\bar{\sigma}$, car la correspondance $\sigma \rightarrow \bar{\sigma}$ est un homomorphisme injectif de groupe.

Tout cela est facile à vérifier : à toute bonne permutation σ correspond un automorphisme du corps de rupture, laissant K fixe, que l'on notera aussi σ .

BONNE

Un σ
K-auton

Mais, rupture
puis $P(\sigma)$
la racine
racines σ

Récap
que l'on
contexte,
exemples

On pe

• c'est
respecten
du group
degré de

• c'est
de basé;
corps de
automor

On l'a
l'équation
 $G(P|K)$, s
ici encore

on trouverait pour

$$\frac{2}{2} = 1$$

ient de l'anneau de
($a_1, \dots, a_m$). Il est
eaux :

eulement si, tout
 π).
is $K[X_1, \dots, X_m]$
 α_i . Les « bonnes »

0
entre les racines. Il
que Σ_m .

ême, toute bonne

as racines sont :

a_m . Les « bonnes »
corps de rupture.
s
car il s'obtient par

σ^{-1} est aussi une
respond est inverse

e $\sigma \rightarrow \bar{\sigma}$ est un

n σ correspond un
on notera aussi σ .

Un automorphisme d'une extension de K laissant K fixe s'appelle un **K-automorphisme** de l'extension.

Mais, réciproquement, si l'on part d'un K-automorphisme φ du corps de rupture de P sur K et si x est une racine de P , l'égalité $P(x) = 0$ donne $\varphi P(x) = 0$ puis $P(\varphi(x)) = 0$ car les coefficients de P sont fixes par φ . Dès lors l'image $\varphi(x)$ de la racine x est encore une racine de P et φ définit bien une permutation des racines qui respecte bien sûr les relations rationnelles (pourquoi ?).

Récapitulons : à tout polynôme $P \in K[X]$ on associe un groupe, noté $G(P|K)$, que l'on appelle **groupe de Galois** de P sur K . Si le corps de base est clair dans le contexte, on écrira simplement $G(P)$; ce corps de base sera souvent $\mathbb{Q}$ dans nos exemples.

On peut le voir de deux manières :

- c'est le groupe des bonnes permutations des racines du polynôme, celles qui respectent les relations rationnelles entre les racines ; c'est alors un sous-groupe du groupe symétrique Σ_m où m est le nombre de racines de P (donc inférieur au degré de P), et son ordre divise m !;

- c'est le groupe des automorphismes du corps de rupture laissant fixe le corps de base ; c'est alors un sous-groupe du groupe de tous les automorphismes du corps de rupture (quand le corps de base est $\mathbb{Q}$, on trouve d'ailleurs *tous* les automorphismes du corps de rupture).

On l'appelle indifféremment groupe de Galois, sur K , du polynôme P , de l'équation $P(X) = 0$ ou du corps de rupture H de P sur K . On le note donc soit $G(P|K)$, soit $G(H|K)$, cette dernière notation insistant sur le second point de vue ; ici encore, $G(H)$ suffira si K est clair dans le contexte.

- Sur un corps algébriquement clos, tout groupe de Galois est réduit à l'identité.

- Pour un polynôme de degré 2, le groupe de Galois est d'ordre 1 ou 2 suivant que le polynôme est réductible ou non.

- Le groupe de Galois de P est le même que celui de P^n , et celui d'un polynôme T est le même que celui du produit de ses facteurs premiers deux à deux distincts. Bref, on peut « supprimer les exposants des facteurs ».

- Tout automorphisme d'un corps laisse fixe le sous-corps premier. En particulier, si L contient $\mathbb{Q}$, tout automorphisme de L est un $\mathbb{Q}$ -automorphisme.

- On montrera plus tard que le groupe de Galois de l'équation générale de degré n est Σ_n tout entier : toutes les permutations sont « bonnes » car les seules relations rationnelles entre les racines sont symétriques.

- On ne sait pas si, pour tout groupe fini, il existe un polynôme sur $\mathbb{Q}$ dont il est le groupe de Galois.

- Pour un polynôme réel sans racines réelles, le groupe de Galois sur $\mathbb{R}$ est formé de l'identité de $\mathbb{C}$ et la conjugaison complexe.

Un exemple.

Reprenons le polynôme

$$(X^2 - 2)(X^2 - 3) \in \mathbb{Q}[X]$$

dont le corps de rupture est $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ et utilisons le fait que $x = \sqrt{2} + \sqrt{3}$ est un élément primitif.

On a montré (voir p. 97) que le polynôme minimum M_x de x sur $\mathbb{Q}$ est de degré 4, ses quatre racines étant $\pm \sqrt{2} \pm \sqrt{3}$. Comme tout automorphisme du corps de rupture laisse fixe le polynôme M_x , l'image de x est encore une racine de M_x , c'est donc l'une de ces quatre valeurs.

Réciproquement soit y l'une des racines de M_x . Alors y est dans

$$\mathbb{Q}(x) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

donc $\mathbb{Q}(y)$ est inclus dans $\mathbb{Q}(x)$ et, par suite, il y a égalité pour raisons de degrés. Dès lors, la transformation de $\mathbb{Q}(x)$ qui envoie la base $(1, x, x^2, x^3)$ sur la base $(1, y, y^2, y^3)$ est $\mathbb{Q}$ -linéaire et bijective; de plus, elle respecte la multiplication, car le produit se fait en prenant les deux polynômes de degré inférieur à 3 et le reste de la division euclidienne par M_x de leur produit.

Conclusion : à tout choix de y correspond un $\mathbb{Q}$ -automorphisme de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, le groupe de Galois est d'ordre 4. Faisons la liste des choix de y , en écrivant côte à côte la bonne permutation des racines $(\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3})$ et l'écriture cyclique de la permutation.

$\sqrt{2} + \sqrt{3}$	$(\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3})$	id
$\sqrt{2} - \sqrt{3}$	$(\sqrt{2}, -\sqrt{2}, -\sqrt{3}, \sqrt{3})$	(3 4)
$-\sqrt{2} + \sqrt{3}$	$(-\sqrt{2}, \sqrt{2}, \sqrt{3}, -\sqrt{3})$	(1 2)
$-\sqrt{2} - \sqrt{3}$	$(-\sqrt{2}, \sqrt{2}, -\sqrt{3}, \sqrt{3})$	(1 2)(3 4)

Le groupe de Galois $G(\mathbb{Q}(\sqrt{2}, \sqrt{3}))$ est un groupe d'ordre 4, formé de l'identité, de deux éléments d'ordre 2 qui commutent et de leur produit : c'est le produit cartésien des deux groupes cycliques engendrés par (1, 2) et (3, 4). On écrira

$$G(X^4 - 5X^2 + 6) = C_2 \times C_2$$

c'est le produit cartésien des groupes de Galois des facteurs

La déterminer

L'exemple du groupe de Galois du corps de rupture. D'après le caractère en caractéristique 2 (cas...).

On part de $(a_1, \dots, a_m)$

Soit q son degré. Dans ce cas, M_x est alors

Par conséquent cette image

Ceci dit, pour la clôture algébrique

S'il existe qu'une éventuelle pour un $R \in K(x)$ s'écrit F multiples de correspondance pour ces conditions

et c'est bien. Ce sera un corps de clôture algébrique $K(x)$; mais K par l'isomorphisme des racines de P

$(X^2 - 2)$ et $(X^2 - 3)$. Les quatre automorphismes du corps $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sont :

$$\begin{aligned}\lambda_0 + \lambda_1 \sqrt{2} + \lambda_2 \sqrt{3} + \lambda_3 \sqrt{6} &\rightarrow \lambda_0 + \lambda_1 \sqrt{2} + \lambda_2 \sqrt{3} + \lambda_3 \sqrt{6} \\ &\rightarrow \lambda_0 + \lambda_1 \sqrt{2} - \lambda_2 \sqrt{3} - \lambda_3 \sqrt{6} \\ &\rightarrow \lambda_0 - \lambda_1 \sqrt{2} + \lambda_2 \sqrt{3} - \lambda_3 \sqrt{6} \\ &\rightarrow \lambda_0 - \lambda_1 \sqrt{2} - \lambda_2 \sqrt{3} + \lambda_3 \sqrt{6}\end{aligned}$$

les λ_i étant dans le corps de base $\mathbb{Q}$.

La détermination du groupe de Galois.

L'exemple ci-dessus indique la marche à suivre pour la détermination du groupe de Galois, au moins quand il existe un élément primitif dans le corps de rupture. D'après le théorème de l'élément primitif, c'est forcément le cas si l'on est en caractéristique nulle, ce que l'on supposera ici (bien que ce soit loin d'être le seul cas...).

On part donc d'un polynôme $P \in K[X]$ de degré n , et on numérote $(a_1, \dots, a_m)$ l'ensemble de ses racines. Le corps de rupture est

$$K(a_1, \dots, a_m).$$

Soit q son degré (inférieur à m !).

Dans ce corps de rupture, soit x un élément primitif; son polynôme minimum M_x est alors de degré q et il est fixe par tout K -automorphisme de

$$K(a_1, \dots, a_m) = K(x).$$

Par conséquent, l'image de x par un tel K automorphisme est une racine de M_x , et cette image détermine l'automorphisme, car le corps est engendré par x sur K .

Ceci dit, peut-on prendre pour image de x une racine *arbitraire* y de M_x (dans la clôture algébrique $\bar{K}$ de K) ?

S'il existe un K -automorphisme de $K(x)$ transformant x en y , ce ne peut être qu'une éventuelle « substitution de x par y » : tout élément de $K(x)$ s'écrit $R(x)$ pour un $R \in K[X]$, son image devra être $R(y)$. Mais attention : un élément de $K(x)$ s'écrit $R(x)$ pour *plusieurs* polynômes $R \in K[X]$, différant entre eux par des multiples de M_x . La valeur $R(y) \in K(y)$ est-elle la même pour tous les polynômes R correspondant à une même valeur de $R(x) \in K(x)$? Oui, car $M_x(y)$ est nul : on voit pourquoi il est nécessaire que x et y aient même polynôme minimum. Dans ces conditions, l'application suivante est bien définie

$$\begin{aligned}\varphi : R(x) &\rightarrow R(y) \\ K(x) &\rightarrow K(y)\end{aligned}$$

et c'est bien sûr un isomorphisme de corps, laissant fixe le corps K .

Ce sera un K -automorphisme de $K(x)$ si, et seulement si, $K(y)$, sous-corps de la clôture algébrique $\bar{K}$ de K , est *égal* à $K(x)$. Il suffit pour cela que $K(y)$ contienne $K(x)$; mais $K(x)$ est engendré par les racines de P et ces racines sont permutées par l'isomorphisme φ puisque P est fixe. Dès lors $K(y)$, image de φ , contient les racines de P et contient donc $K(x)$: il lui est égal.

D'ailleurs, $K(x)$ et $K(y)$ sont tous deux naturellement isomorphes au quotient $K[X]/M_x$, et l'application φ n'est autre que la composée $K(x) \rightarrow K[X]/M_x \rightarrow K(y)$ de deux isomorphismes.

On vient d'établir (au moins en caractéristique nulle, pour utiliser le théorème de l'élément primitif) une bijection naturelle entre

- le groupe de Galois $G(P)$, formé des bonnes permutations des racines de P ;
- les racines du polynôme minimum d'un élément primitif du corps de rupture.

Or, le nombre de racines d'un polynôme irréductible est égal au degré car les racines sont simples. D'où le résultat fondamental :

L'ordre du groupe de Galois d'un polynôme est le degré de son corps de rupture.

Quelques remarques.

1° Pour un polynôme de degré n , on savait que le corps de rupture avait un degré inférieur à $n!$. Il y a mieux : comme ce degré est l'ordre d'un sous-groupe de Σ_n , il divise $n!$.

2° D'après la manière dont est engendré le groupe symétrique, le groupe de Galois d'un polynôme ayant n racines sera tout le groupe symétrique Σ_n (c'est-à-dire que toutes les permutations seront bonnes) dès que seront bonnes les permutations d'une des catégories suivantes :

- toutes les transpositions ;
- toutes les transpositions échangeant une racine donnée avec les autres ;
- une transposition et un cycle de longueur n (c'est-à-dire portant sur toutes les racines).

Dans ces conditions, les seules relations rationnelles vérifiées par les racines seront les symétriques.

3° Il est clair que tous les exemples que l'on étudiera seront truqués à un degré plus ou moins important, pour la simple raison que la détermination du groupe de Galois d'une équation « au hasard » est un travail surhumain. « Nous estimons que bien habile serait le calculateur qui, après trois mois de labeur assidu, déterminerait le groupe d'une équation numérique du cinquième degré » (G. Verriest, in *Évariste Galois*, Gauthier-Villars, 1934).

On verra plus loin divers trucs pour avoir des renseignements sur les groupes de Galois.

4° Si P divise T dans $K[X]$, toute bonne permutation des racines de T donne, par restriction, une bonne permutation des racines de P , d'où un homomorphisme de $G(T)$ dans $G(P)$.

On montrera plus tard (voir p. 167) qu'il est surjectif : toute bonne permutation des racines d'un facteur de T se prolonge en une des racines de T .

Il en résultera :

$$P \text{ divise } T \Rightarrow G(P) \text{ est un quotient de } G(T).$$

Le cas d'un

Dans le

on a trouvé
Galois des

Partons de
Par tout K
même pour
permutation
restrictions.
mes de grou

Toute rac
Mais il n'a a
des relations
de S et une

Tout ce qu
sous-groupe

omorphes au quotient
que la composée

utiliser le théorème

s des racines de P;
nitif du corps de

al au degré car les

est le degré de son

rupture avait un
d'un sous-groupe

ique, le groupe de
étrique Σ_n (c'est-à-
seront bonnes les

avec les autres;
portant sur toutes

ées par les racines

truqués à un degré
ination du groupe
rhumain. « Nous
ois mois de labeur
cinquième degré »

nts sur les groupes

acines de T donne,
un homomorphi-

tif : toute bonne
des racines de T.

Le cas d'un polynôme réductible.

Dans le cas de

$$P = (X^2 - 2)(X^2 - 3),$$

on a trouvé que le groupe de Galois de P est le produit cartésien des groupes de Galois des deux facteurs. Il ne faudrait (malheureusement) pas généraliser.

Partons en effet d'un polynôme $P = ST$, produit de deux polynômes S et T. Par tout K-automorphisme, l'image d'une racine de S reste racine de S, et de même pour T, ce qui signifie que tout $\sigma \in G(P)$ donne par restriction une bonne permutation des racines de S et une des racines de T. Appelons σ_S et σ_T ces restrictions. Les deux applications $\sigma \rightarrow \sigma_S$ et $\sigma \rightarrow \sigma_T$ sont des homomorphismes de groupes, d'où l'homomorphisme de groupes suivant :

$$\begin{aligned} \sigma &\rightarrow (\sigma_S, \sigma_T) \\ G(P) &\rightarrow G(S) \times G(T). \end{aligned}$$

Toute racine de P étant racine de S ou de T, cet homomorphisme est injectif. Mais il n'a aucune raison d'être surjectif, car les racines de S et T peuvent avoir des relations « entre elles » qui empêchent qu'une bonne permutation des racines de S et une des racines de T en donne une des racines de $P = ST$.

- Le cas le plus flagrant est celui où S et T sont égaux : le groupe de Galois de $P = S^2$ sur K est égal à celui de S, non à son carré cartésien.

- Même en dehors de ce cas...

Prenons ainsi

$$(X^2 - 2)(X^2 - 8)$$

au lieu de

$$(X^2 - 2)(X^2 - 3).$$

Les racines sont $\sqrt{2}$, $-\sqrt{2}$, $2\sqrt{2}$, $-2\sqrt{2}$ et on ne peut échanger les deux premières sans échanger les deux dernières (alors qu'on le pouvait quand ces dernières étaient $\sqrt{3}$ et $-\sqrt{3}$). Autrement dit, la seule bonne permutation autre que l'identité est la transposition *simultanée* des deux premières et des deux dernières. D'où

$$\begin{aligned} G((X^2 - 2)(X^2 - 8)) &= C_2 \\ &\neq G(X^2 - 2) \times G(X^2 - 8) = C_2 \times C_2. \end{aligned}$$

Le corps de rupture est d'ailleurs $\mathbb{Q}(\sqrt{2})$, de degré 2.

Tout ce que l'on peut dire, c'est que le groupe de Galois d'un produit est un sous-groupe du produit cartésien des groupes de Galois.

On peut dire plus dans le cas où il y a une racine de S qui n'est pas racine de T . Car alors aucun élément de $G(P)$ ne la transformera en une racine donnée de T . Une telle décomposition de P existera toujours dès que P aura deux facteurs premiers au moins.

Introduisons alors la notion suivante : un sous-groupe G de Σ_n est dit **transitif** si, quel que soit le couple d'indices (i, j) , il existe un élément de G transformant i en j .

Ainsi, parmi les sous-groupes propres de Σ_3 , seul le groupe alterné A_3 est transitif. Car le sous-groupe formé de id et de la permutation $(1\ 2)$, par exemple, n'a aucun élément transformant 1 en 3 .

On vient de montrer que si P est égal à ST où il y a une racine de S qui n'est pas racine de T , alors le groupe de Galois de P n'est pas transitif.

La conclusion est donc vraie pour tout polynôme P non primaire, c'est-à-dire non puissance d'un polynôme premier.

Et que se passe-t-il si S et T ont mêmes racines, le cas extrême étant celui où ils sont égaux ? Dans ce dernier cas, $G(P)$ peut être transitif : il suffit de prendre $G(X^2)$, la seule racine est 0 , et il est clair que $G(X^2) = \text{id}$ est transitif sur (0) .

Mais si, au lieu de considérer $G(P)$ comme un groupe de permutations de l'ensemble des racines, on le considère comme un groupe de permutations de la famille des racines (donc un sous-groupe de Σ_n où n est le degré de P), alors dans tous les cas on écrit la famille des racines de $P = ST$ comme

$$(a_1, \dots, a_n, b_1, \dots, b_t)$$

où les a_i sont la famille des racines de S et les b_i celle des racines de T . Dans ces conditions, aucun élément de $G(P)$ ne transformera un a_i en un b_j .

La famille des racines de X^2 est $(0, 0)$, et $G(X^2) = \text{id}$ n'est pas transitif sur $(0, 0)$.

Le groupe de Galois d'un polynôme réductible n'est pas transitif sur la famille de ses racines.

Et en dehors du cas où le polynôme est primaire, on peut remplacer « famille » par « ensemble ». On verra plus loin la réciproque (voir p. 165).

Le cas des corps finis.

On a montré que le théorème de l'élément primitif s'applique aussi dans le cas des corps finis, donc là aussi le degré de l'extension est l'ordre du groupe de Galois.

Rappelons aussi qu'un corps fini a un cardinal de la forme p^n , avec p premier (sa caractéristique), et que c'est alors le corps de rupture de $X^{p^n} - X$ sur $\mathbb{Z}/p$. Le corps

de Galois (compter n :

Une tran

- c'est un
- formule du
- il est ir

- il est bi
- c'est ur

(car le corps

En conclu
le groupe de

Dans ces
Galois est u
rupture (car
groupe d'un

On verra

Exercices.

1. Étudie

2. Que p
polynô

3. Si L e
 K -hon
On po
l'éléme

4. Tout
autom

5. Étudie
partici

as racine de T.
 e donnée de T.
 deux facteurs

est dit **transitif**
 transformant i

seul le groupe
 de id et de la
 t transformant

S qui n'est pas
 ire, c'est-à-dire

tant celui où ils
 ffrit de prendre
 ansitif sur (0).

rmutations de
 mutations de la
 e P), alors dans

de T. Dans ces
 : b_j .

= id n'est pas

pas transitif sur

acer « famille »
).

ussi dans le cas
 du groupe de

ec p premier (sa
 ir $\mathbb{Z}/p$. Le corps

de Galois $CG(p^n)$ est de degré n sur le sous-corps premier $\mathbb{Z}/p$, donc il doit compter n automorphismes.

Une transformation importante de $CG(p^n)$ est $\varphi : x \rightarrow x^p$. En effet :

- c'est un endomorphisme de corps (la compatibilité avec l'addition utilise la formule du binôme et le fait que p est nul dans le corps)
- il est injectif :

$$x^p = 1 \Rightarrow x^{p \cdot p^{n-1}} = 1 \Rightarrow x^{p^n} = 1 \Rightarrow x = 1$$

- il est bijectif (car les ensembles sont finis)
- c'est un automorphisme d'ordre n : pour $q \geq 1$, on vérifie

$$\varphi^q = \text{id} \Rightarrow x^{p^q} = x \text{ pour tout } x \Rightarrow q \geq n$$

(car le corps est alors contenu dans le corps de rupture de $X^{p^n} - X$, de cardinal p^q).

En conclusion, les n puissances de φ sont les seuls automorphismes de $CG(p^n)$, le groupe de Galois (sur le sous-corps premier $\mathbb{Z}/p$) est cyclique engendré par φ :

$$G[CG(p^n)] = C_n.$$

Dans ces conditions, si P est un polynôme sur le corps fini K , son groupe de Galois est un sous-groupe du groupe de tous les automorphismes du corps de rupture (car ce sont les automorphismes laissant K fixe), c'est donc un sous-groupe d'un groupe cyclique.

Sur un corps fini, le groupe de Galois de tout polynôme est cyclique.

On verra des précisions plus loin (voir p. 166).

Exercices.

1. Étudier, sur $\mathbb{Q}$, les groupes de Galois de

$$\begin{aligned} X^3 + 2X + 1 \\ X^4 + X^2 + X + 1. \end{aligned}$$

2. Que peut-on dire du groupe de Galois d'un polynôme pair (c'est-à-dire un polynôme en X^2) ?
3. Si L est une extension de degré fini de K , le degré $L:K$ est le nombre de K -homomorphismes de L dans la clôture algébrique de K (qui contient bien sûr L). On pourra commencer par une extension simple, puis utiliser le théorème de l'élément primitif.
4. Tout K -endomorphisme d'une extension algébrique de K est un K -automorphisme.
5. Étudier le groupe de Galois de $(X^2 - 2)(X^2 - 3)$ sur divers corps finis, en particulier les $\mathbb{Z}/p$.

Quelques exemples de groupes de Galois

La détermination pratique du groupe de Galois d'un polynôme donné n'est pas toujours facile. Quelques remarques sont souvent utiles.

- Si un polynôme de degré n possède de manière évidente au moins m racines dans le corps de base, son groupe de Galois est sous-groupe de Σ_{n-m} .
- Le degré du corps de rupture est souvent relativement facile à déterminer, et il donne l'ordre du groupe de Galois ; si p est cet ordre, le problème revient à trouver p bonnes permutations des racines, ou encore p automorphismes conservant le corps de base. On utilisera à cet effet la propriété suivante : l'image de tout élément par un tel automorphisme est encore racine de son polynôme minimum. Cette remarque permet de « limiter » le nombre de ces automorphismes quand on connaît des éléments engendrant le corps de rupture.
- Si le corps de rupture est donné *a priori* comme engendré par plusieurs éléments, on peut commencer par considérer les automorphismes conservant certains de ces éléments. Par exemple, si ledit corps de rupture est $\mathbb{Q}(\alpha, \beta)$, les automorphismes laissant fixe α , c'est-à-dire les $\mathbb{Q}(\alpha)$ -automorphismes, sont en nombre égal au degré de β sur $\mathbb{Q}(\alpha)$; on passera ensuite aux automorphismes qui ne laissent pas fixe α , ils transforment alors α en une autre racine de son polynôme minimum sur $\mathbb{Q}$.

Des exemples plus ou moins au hasard.

- Pour tout polynôme réel de degré 2 irréductible sur $\mathbb{R}$ (c'est-à-dire à discriminant strictement négatif), le corps de rupture est $\mathbb{R}(i) = \mathbb{C}$.
Le groupe de Galois est formé de l'identité et de la conjugaison complexe

$$a + bi \rightarrow a - bi.$$

- Prenons maintenant un polynôme rationnel sans racine dans $\mathbb{Q}$. Le corps de rupture est de degré 2, formé de l'identité et d'un autre automorphisme. Deux cas se présentent, suivant que le discriminant Δ (qui n'a pas de racine carrée dans $\mathbb{Q}$) est négatif ou positif.

Cas $\Delta < 0$: les deux racines sont complexes conjuguées, le corps de rupture $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(i\sqrt{-\Delta})$ est non réel, et l'automorphisme correspondant à l'échange des deux racines est la trace sur $\mathbb{Q}(\sqrt{\Delta})$ de la conjugaison complexe, soit

$$a + ib\sqrt{-\Delta} \rightarrow a - ib\sqrt{-\Delta}$$

(a et b dans $\mathbb{Q}$, et $\sqrt{-\Delta}$ dans $\mathbb{R}$).

Cas $\Delta > 0$: ici les deux racines sont réelles, le corps de rupture $\mathbb{Q}(\sqrt{\Delta})$ est réel et l'automorphisme autre que l'identité est

$$a + b\sqrt{\Delta} \rightarrow a - b\sqrt{\Delta} \quad (a \text{ et } b \text{ dans } \mathbb{Q}).$$

Contrairement au premier cas, cet automorphisme ne se prolonge pas en automorphisme de $\mathbb{C}$ (ni de $\mathbb{R}$ d'ailleurs).

- Le groupe de Galois de $X^3 - 1$ sur $\mathbb{Q}$ est d'ordre 2, formé de l'identité et de la trace de la conjugaison complexe, soit

$$a + bj \rightarrow a + bj^2$$

ou

$$u + vi\sqrt{3} \rightarrow u - vi\sqrt{3}$$

suivant que l'on prend j ou $i\sqrt{3}$ comme élément primitif.

- Les racines de $1 + X^2 + X^4$ sont les racines carrées de j et j^2 , elles forment donc la suite $(-j^2, -j, j, j^2)$. Le corps de rupture sur $\mathbb{Q}$ est

$$\mathbb{Q}(j) = \mathbb{Q}(\sqrt{-3})$$

donc le groupe de Galois est d'ordre 2, c'est le même que pour $1 + X + X^2$ ou pour $X^3 - 1$.

La seule bonne permutation autre que l'identité correspond à $j \rightarrow j^2$, c'est-à-dire à la conjugaison complexe, c'est donc

$$(-j^2, -j, j, j^2) \rightarrow (-j, -j^2, j^2, j)$$

que l'on écrit

$$(1 \ 2)(3 \ 4) \text{ en notation cyclique.}$$

- On a déjà vu que le réel $x = \sqrt[3]{1 - \sqrt{2}}$ est racine du polynôme rationnel

$$(X^3 - 1)^2 - 2 = X^6 - 2X^3 - 1$$

ce polynôme étant irréductible sur $\mathbb{Q}$.

Les racines complexes de

$$P = X^6 - 2X^3 - 1$$

Exemples de Galois

me donné n'est

moins m racines
le Σ_{n-m}

à déterminer, et
blème revient à
utomorphismes
divante : l'image
son polynôme
s automorphis-
pture.

ré par plusieurs
mes conservant
est $\mathbb{Q}(\alpha, \beta)$, les
hismes, sont en
morphisms qui
racine de son

le sur $\mathbb{R}$ (c'est-à-
s de rupture est

de la conjugaison

is racine dans $\mathbb{Q}$.
l'identité et d'un
s, suivant que le
 $\mathbb{Q}$) est négatif ou

sont $x = \sqrt[3]{1 - \sqrt{2}}$, $y = \sqrt[3]{1 + \sqrt{2}} = -\frac{1}{x}$ et leurs produits par j et j^2 .

Le corps de rupture de P est donc

$$\mathbb{Q}(x, j) = \mathbb{Q}(x, \sqrt{-3})$$

il est de degré 12 car x est de degré 6 sur $\mathbb{Q}$ et $\sqrt{-3}$ est racine de $X^2 + 3$ qui est irréductible sur le corps réel $\mathbb{Q}(x)$. Le groupe de Galois $G(P)$ est donc d'ordre 12, il n'y a que douze bonnes permutations parmi les $6! = 720$ permutations des six racines

$$\left(x, jx, j^2x, -\frac{1}{x}, -\frac{j}{x}, -\frac{j^2}{x}\right).$$

Pour voir de plus près la structure de ce groupe d'ordre 12, on remarque qu'il y a six $\mathbb{Q}(\sqrt{-3})$ -automorphismes (ceux qui conservent j et transforment x en l'une des six racines) et six automorphismes transformant j en j^2 .

On peut aussi partager autrement le groupe, en coupant « naturellement » la famille des racines en deux, soit

$$A = (x, jx, j^2x) \quad \text{et} \quad B = \left(-\frac{1}{x}, -\frac{j}{x}, -\frac{j^2}{x}\right)$$

et en remarquant que les éléments du groupe de Galois qui laissent A stable sont les $\mathbb{Q}(\sqrt{2})$ -automorphismes, puisque x, jx, j^2x sont les racines de

$$X^3 - (1 - \sqrt{2}).$$

Ils forment donc un sous-groupe H qui est le groupe de Galois du polynôme sur $\mathbb{Q}(\sqrt{2})$, c'est-à-dire encore $G(\mathbb{Q}(x, j) | \mathbb{Q}(\sqrt{2}))$. Comme x est de degré 3 sur $\mathbb{Q}(\sqrt{2})$ et j de degré 2 sur le corps réel $\mathbb{Q}(\sqrt{2}, x)$, l'extension $\mathbb{Q}(x, j)$ est de degré 6 sur $\mathbb{Q}(\sqrt{2})$, donc notre sous-groupe H est d'ordre 6, c'est forcément Σ_3 tout entier. Les douze éléments du groupe de Galois sont alors les six éléments de H et leurs six produits par un élément hors de H , par exemple par la permutation σ qui conserve j et transforme x en $-\frac{1}{x}$.

Le groupe de Galois d'un polynôme de degré 3.

Soit P un polynôme de degré 3 sur un corps K . Alors

- P est irréductible si, et seulement si, il n'a pas de racine dans K ;
- si P est réductible, il possède 1 ou 3 racines dans K (en tenant compte des ordres de multiplicité);

et leurs produits

-3 est racine de $P(x)$. Le groupe de Galois est l'un des six racines

de degré 12, on considère les six racines

en coupant x , soit

$$\left(\frac{j}{x}, -\frac{j^2}{x} \right)$$

le groupe de Galois qui agit sur les racines, puisque

le groupe de Galois du $\mathbb{Q}(x, j) / \mathbb{Q}(x, \sqrt{2})$ est d'ordre 2 sur le corps réel $\mathbb{Q}(\sqrt{2})$, donc le groupe de Galois est Σ_3 tout entier, ont alors les six racines hors de H , par j et transforme

- le groupe de Galois $G(P)$ est un sous-groupe de Σ_3 ;
- les seuls sous-groupes de Σ_3 autres que Σ_3 et $\{id\}$ sont le groupe alterné A_3 , d'ordre 3, et les trois groupes d'ordre 2 formés par l'identité et une transposition (chacun est bien sûr isomorphe à C_2 , cyclique d'ordre 2); seuls Σ_3 et A_3 sont transitifs.

D'où les premières équivalences :

$$G(P) = id \Leftrightarrow P \text{ est totalement factorisable sur } K$$

$$G(P) = C_2 \Leftrightarrow P \text{ possède une, et une seule, racine dans } K.$$

Dans ce dernier cas, l'échange des racines hors de K est la seule bonne permutation autre que l'identité.

Les deux cas restant correspondent donc aux polynômes de degré 3 irréductibles sur K : le groupe de Galois est alors A_3 ou Σ_3 , et il nous faut caractériser les deux circonstances.

Partons donc de P irréductible sur K , et prenons-le directement sous la forme

$$P = X^3 + pX + q.$$

Notons a, b, c ses racines, toutes hors de K et deux à deux distinctes (à cause de l'irréductibilité).

Le corps de rupture est alors engendré sur K par deux racines; mais en développant l'égalité

$$(b - c)^2 = (b + c)^2 - 4bc$$

à l'aide des fonctions symétriques élémentaires, on arrive à (voir p. 55)

$$(b - c)^2 = -3a^2 - 4p$$

$$a = \frac{3q}{(b - c)^2 + p}$$

égalités qui montrent que tout corps contenant $b - c$ contient a , donc aussi $b + c$, donc enfin b et c .

En conclusion, le corps de rupture de $X^3 + pX + q$ est l'extension simple $K(b - c)$, égale encore à

$$K(\sqrt{-3a^2 - 4p}).$$

L'ordre du groupe de Galois est égal au degré de $x = \sqrt{-3a^2 - 4p}$ sur K ; ce degré devra être 3 ou 6, le groupe de Galois correspondant étant respectivement A_3 et Σ_3 .

On trouve facilement une équation dont x^2 est racine, en effectuant, dans l'équation aux carrés de $P(X) = 0$, la substitution de X par $-\frac{X + 4p}{3}$. Plus précisément, l'équation aux carrés est

$$X(X + p)^2 - q^2 = 0,$$

soit

$$X^3 + 2pX^2 + p^2X - q^2 = 0,$$

dans K ;
tenant compte des

et la substitution de X par $-\frac{X+4p}{3}$ donne

$$\begin{aligned} -\frac{X+4p}{3} \left(\frac{-X-p}{3} \right)^2 - q^2 &= 0 \\ (X+4p)(X+p)^2 + 27q^2 &= 0 \\ X(X+3p)^2 + 4p^3 + 27q^2 &= 0 \end{aligned}$$

Autrement dit, l'élément primitif

$$x = b - c = \sqrt{-3a^2 - 4p}$$

est racine du polynôme de degré 6

$$Q = X^2(X^2 + 3p)^2 + 4p^3 + 27q^2.$$

Tout va dépendre de l'irréductibilité de ce polynôme : s'il est irréductible, le corps de rupture est de degré 6 et le groupe de Galois est Σ_3 ; sinon, c'est A_3 .

Notons que les racines de Q sont les six différences deux à deux des racines.

Le discriminant au degré 3 et son rôle.

Au point où on en est, on voit réapparaître la fameuse expression

$$\Delta = -4p^3 - 27q^2$$

appelée **discriminant** du polynôme

$$P = X^3 + pX + q.$$

C'est l'opposé du produit des différences deux à deux des racines, car c'est l'opposé du terme constant $Q(0)$ de Q . En d'autres termes, on peut écrire

$$\Delta = (a-b)^2(a-c)^2(b-c)^2$$

et la nullité de Δ équivaut, dans le cas général, à l'existence d'une racine multiple (bien entendu la question ne se pose pas ici car notre polynôme est supposé irréductible).

Revenons au problème de l'irréductibilité, sur K , de

$$Q = X^2(X^2 + 3p)^2 - \Delta.$$

- Si Δ possède une racine carrée dans K , la décomposition

$$Q = (X(X^2 + 3p) + \sqrt{\Delta}) (X(X^2 + 3p) - \sqrt{\Delta})$$

dans $K[X]$ montre que Q est réductible, donc le groupe de Galois est A_3 .

- Montrons réciproquement que, si Q est réductible sur K , alors Δ possède une racine carrée dans K . Notons d'abord que, si Q est réductible, il a forcément un facteur irréductible de degré 3. Posons donc $Q = RS$, avec R irréductible de

degré 3 sur K . L'égalité $Q(X) = Q(-X)$ donne

$$R(X)S(X) = R(-X)S(-X)$$

d'où l'on déduit que $R(X)$ divise $R(-X)$ ou $S(-X)$.

En prenant les coefficients dominants de R et S égaux à 1, ce que l'on peut toujours faire, il reste soit l'égalité

$$R(X) = -S(-X),$$

soit l'égalité

$$R(X) = -R(-X).$$

Le dernier cas donne $R(0) = 0$, d'où $Q(0) = 0$ et $\Delta = 0$, ce qui est à exclure comme on l'a signalé (irréductibilité de P). Reste donc la condition $R(X) = -S(-X)$, d'où

$$Q(X) = -R(X)R(-X)$$

qui donne

$$Q(0) = -(R(0))^2$$

et Δ est le carré de $R(0) \in K$.

Autrement dit, dans le cas irréductible, ou bien Δ n'a pas de racine carrée dans K et alors le corps de rupture est de degré 6 et le groupe de Galois est Σ_3 , ou bien Δ a une racine carrée dans K et le corps de rupture est de degré 3, le groupe de Galois étant A_3 .

Dans ce dernier cas, chaque racine est élément primitif du corps de rupture.

Dans le premier cas ($\sqrt{\Delta} \notin K$) toutes les permutations des racines sont bonnes, alors que, dans le second cas, les transpositions sont des mauvaises permutations : on le voit directement en considérant la relation rationnelle suivante sur K

$$(a-b)(b-c)(a-c) = \sqrt{\Delta}$$

qui n'est pas respectée par une transposition de deux racines.

Si l'on veut compléter le rôle du discriminant pour *tous* les cas, il convient d'examiner aussi les cas où

$$P = X^3 + pX + q$$

est réductible, ce qui correspond aux groupes de Galois $\{id\}$ ou C_2 .

- $G(P) = \{id\}$: alors a, b, c sont dans K , et

$$(a-b)(b-c)(c-a)$$

est une racine carrée de Δ dans K .

- $G(P) = C_2$: il y a une racine dans K , soit a , et deux hors de K , racines du polynôme de degré 2 irréductible sur K

$$\frac{P(X)}{X-a} = X^2 + uX + v.$$

En ce cas $(b - c)^2$ est égal à $u^2 - 4v$, donc sans racine carrée dans K , alors que $a - b$ et $a - c$ ont pour produit

$$a^2 - (b + c)a + bc$$

qui est dans K : donc Δ est égal à

$$(a^2 + ua + v)^2(u^2 - 4v)$$

et n'a pas de racine carrée dans K .

Si l'on récapitule, on écrira dans tous les cas :

$$\begin{aligned}\sqrt{\Delta} \notin K &\Leftrightarrow G(P) = \Sigma_3 \text{ ou } G(P) = C_2 \\ \sqrt{\Delta} \in K &\Leftrightarrow G(P) = A_3 \text{ ou } G(P) = \text{id.}\end{aligned}$$

Dans le cas irréductible, seule la première partie des seconds membres est à retenir.

Une remarque : si le coefficient de X^2 n'est pas nul, la transformation usuelle permet le calcul du discriminant de

$$X^3 + a_1X^2 + a_2X + a_3.$$

On trouve

$$\Delta = 18a_1a_2a_3 - 4a_1^3a_3 + a_1^2a_2^2 - 4a_2^3 - 27a_3^2.$$

Quelques exemples au degré 3.

- Sur $\mathbb{R}$, une équation de degré 3 a toujours une racine réelle, le groupe de Galois est donc C_2 ou id , ceci suivant que $\Delta = -4p^3 - 27q^2$ est strictement négatif ou non.

Dans le cas $\Delta < 0$ il y a une unique racine réelle, alors que pour $\Delta \geq 0$ il y en a trois, toutes simples, si Δ est non nul, et une double ou une triple si Δ est nul.

- Le discriminant de $1 + X + X^3$ est $\Delta = -4 - 27 = -31$, sans racine carrée dans $\mathbb{Q}$. Comme le polynôme n'a pas de racine dans $\mathbb{Q}$, il y est irréductible, et son groupe de Galois sur $\mathbb{Q}$ est Σ_3 : il y a six automorphismes du corps de rupture (sous-corps de $\mathbb{C}$), correspondant aux six permutations des trois racines complexes.

Le fait que $1 + X + X^3$ n'ait pas de racine rationnelle s'obtient en écrivant que $\frac{p}{q}$ (p et q premiers entre eux) est racine, d'où l'égalité

$$q^3 + pq^2 + p^3 = 0$$

qui montre que p divise q et q divise p .

sur K , alors que

- Les deux polynômes

$$1 - 3X + X^3 \quad \text{et} \quad 1 + 3X + X^3$$

sont irréductibles sur $\mathbb{Q}$, car sans racines (pourquoi ?), leurs discriminants valent 81 et -135 , donc les groupes de Galois sont respectivement A_3 et Σ_3 .

Toute racine du premier est élément primitif de son corps de rupture alors que, pour le second, une racine ne suffit pas : il faut adjoindre aussi $\sqrt{-135}$, ou $i\sqrt{15}$.

- Pour l'équation binôme $X^3 - 2 = 0$ sur K , le discriminant est $-27 \times 4 = -3 \times 6^2$, donc, sur un corps dans lequel 2 n'a pas de racine cubique, le groupe de Galois de $X^3 - 2$ est Σ_3 ou A_3 suivant que -3 n'a pas ou a une racine carrée.

Plaçons-nous sur $\mathbb{Q}$ en appelant $\sqrt[3]{2}$ la racine cubique réelle de 2. Le corps de rupture est $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$, de degré 6 puisque le groupe de Galois est Σ_3 .

Par contre, si le corps de base est

$$K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(j)$$

le groupe de Galois se réduit à A_3 car on impose que j soit fixe et les transpositions des racines ne sont pas des bonnes permutations.

Ainsi, si l'on pose

$$x_1 = \sqrt[3]{2} \quad \text{et} \quad x_2 = j\sqrt[3]{2}$$

l'égalité

$$0 = x_2 - jx_1$$

n'est pas une relation rationnelle sur $\mathbb{Q}$, mais c'en est une sur $\mathbb{Q}(\sqrt{-3})$, et aucune transposition ne la respecte.

- Plus généralement, le discriminant de l'équation binôme $X^3 - \alpha = 0$ est $\Delta = -27\alpha^2$, soit $\Delta = -3(3\alpha)^2$.

On a vu que $X^3 - \alpha$ est irréductible si, et seulement si, le corps de base K ne contient pas de racine cubique de α . Le groupe de Galois est alors Σ_3 si K ne contient pas $\sqrt{-3}$, A_3 si K contient $\sqrt{-3}$ (ou j , ce qui revient au même).

- Dans tous les cas, il est facile de vérifier que le corps de rupture d'un polynôme de degré 3 est engendré par une racine du polynôme et une racine carrée du discriminant.

Groupe de Galois du corps cyclotomique.

On a appelé corps cyclotomique d'indice n sur le corps K le corps engendré par K et les racines n -ièmes de l'unité.

C'est le corps de rupture de $X^n - 1$ sur K , égal à $K(\omega_n)$, où ω_n est une racine n -ième primitive de l'unité sur K .

L'ordre du groupe de Galois est le degré de ω_n sur K .

Dans le cas de $\mathbb{Q}$, on montre que le degré est $\varphi(n)$, nombre d'entiers premiers avec n et inférieurs à n .

En tout cas, tout K -automorphisme de $K(\omega_n)$ est donné par l'image de ω_n qui est une puissance de ω_n dont l'exposant est un entier inversible modulo n . Le groupe de Galois est donc un sous-groupe de $(\mathbb{Z}/n)^*$, groupe multiplicatif des entiers inversibles modulo n , et il est toujours abélien.

Ce sous-groupe peut être propre. C'est le cas bien sûr si K contient déjà les racines n -ièmes de l'unité.

Sur le corps $\mathbb{Q}$, le degré de ω_n est $\varphi(n)$, donc le groupe de Galois de $X^n - 1$ est tout le groupe $(\mathbb{Z}/n)^*$. Mais, même si K ne contient pas toutes les racines, le groupe de Galois peut être sous-groupe propre.

Ainsi, les racines de $X^8 - 1$ sont

$$\pm 1, \pm i, \frac{\pm 1 \pm i}{\sqrt{2}}$$

et le groupe $(\mathbb{Z}/8)^* = \{1, 3, 5, 7\}$ est isomorphe à $C_2 \times C_2$ (car tout élément possède un carré égal à 1).

Les racines primitives sont les quatre dernières, racines de $X^4 + 1$, et le corps de rupture est $\mathbb{Q}(i, \sqrt{2})$.

Sur $\mathbb{Q}$, le groupe de Galois est $C_2 \times C_2$, mais sur $\mathbb{Q}(i)$ c'est C_2 , car i est fixe et la seule bonne permutation autre que l'identité à $\sqrt{2} \rightarrow -\sqrt{2}$.

Un cas particulier est celui où n est premier. En ce cas toutes les racines autres que 1 sont primitives, donc ou bien K en contient une et alors il les contient toutes, ou bien K n'en contient aucune.

Dans cette dernière hypothèse, les racines primitives ont pour polynôme minimum commun

$$1 + X + X^2 + \dots + X^{n-1}$$

elles sont de degré $(n-1)$, et si l'on en choisit une, ω_n , les K -automorphismes correspondent de manière bijective aux images de ω_n , qui sont de la forme ω_n^q avec $q = 1, 2, \dots, (n-1)$, la composition correspondant au produit des exposants modulo n . Le groupe multiplicatif $\mathbb{Z}/n \setminus 0$ est cyclique, d'où :

Si p est premier, le groupe de Galois de $X^p - 1$ sur un corps ne contenant pas toutes les racines p -ièmes de l'unité est cyclique d'ordre $(p-1)$.

Groupe

Comr
équation
binômes

Soit a

une racin
sous-cor,

et le corp
Tout f
qu'un K

Bornor
déterminé
en questio

montre q
modulo n
Bref, l'a
groupe de
groupe cy

En parti
ordre est k

Bien ent
cas « extrê
alors le gro

D'autre
si, le corps
arbitraire c
équivalent à

Groupe de Galois d'une équation binôme.

Comme on l'a vu dans la formulation du problème de la résolution des équations, une importance exceptionnelle est attribuée aux équations dites binômes, de la forme $X^n - a$ et, plus précisément, au cas où n est premier.

Soit $a \in K$; appelons α une racine n -ième de a dans le corps de rupture, et ω_n une racine primitive n -ième de l'unité (par exemple $\omega_n = e^{\frac{2\pi i}{n}}$ dans le cas d'un sous-corps de $\mathbb{C}$). La famille des racines de $X^n - a$ est

$$\alpha, \omega_n \alpha, \omega_n^2 \alpha, \dots, \omega_n^{n-1} \alpha$$

et le corps de rupture est $K(\alpha, \omega_n)$.

Tout K -automorphisme est donné par l'image de α et l'image de ω_n , alors qu'un $K(\omega_n)$ -automorphisme est donné par l'image de α seulement.

Bornons-nous aux $K(\omega_n)$ -automorphismes. Tout $\sigma \in G(K(\alpha, \omega_n) | K(\omega_n))$ est déterminé par $\sigma(\alpha)$ qui est de la forme $\omega_n^q \alpha$. Pour σ et τ dans le groupe de Galois en question, l'égalité

$$\tau\sigma(\alpha) = \omega_n^q \tau(\alpha)$$

montre qu'au produit de deux $K(\omega_n)$ -automorphismes correspond la somme modulo n des exposants de ω_n .

Bref, l'application $\sigma \rightarrow q$ est un homomorphisme injectif de groupes du groupe de Galois dans le groupe additif des entiers modulo n , c'est-à-dire le groupe cyclique d'ordre n .

Sur un corps contenant les racines n -ièmes de l'unité, le groupe de Galois d'une équation binôme de degré n est un sous-groupe du groupe cyclique d'ordre n .

En particulier, ce groupe est lui-même cyclique, d'ordre diviseur de n . Or cet ordre est le degré, sur $K(\omega_n)$, du corps de rupture.

Sur un corps contenant les racines adéquates de l'unité, le degré du corps de rupture d'une équation binôme divise le degré de l'équation.

Bien entendu, le groupe de Galois peut être un sous-groupe propre de C_n ; le cas « extrême » est celui où a possède une racine n -ième dans le corps de base, car alors le groupe de Galois est l'identité.

D'autre part, le groupe de Galois de $X^n - a$ sera C_n tout entier si, et seulement si, le corps de rupture est de degré n . Comme il est engendré par une racine n -ième arbitraire de a , cette racine doit avoir un polynôme minimum de degré n , ce qui équivaut à dire que $X^n - a$ est irréductible.

Sur un corps contenant les racines n -ièmes de l'unité, le groupe de Galois d'une équation binôme de degré n est le groupe cyclique d'ordre n si, et seulement si, elle est irréductible.

Un cas particulier important est celui où le degré est premier.

Si p est premier, les seuls sous-groupes de C_p sont C_p et $\{id\}$, donc le corps de rupture de $X^p - a$ est soit de degré p sur K (et alors le polynôme est irréductible), soit égal à K (et alors K contient une racine p -ième de a , donc toutes).

Si p est premier et si a n'a pas de racine p -ième dans un corps K contenant les racines p -ièmes de l'unité, le groupe de Galois de $X^p - a$ est cyclique d'ordre p .

En ce cas, le groupe de Galois est engendré par un cycle de longueur p .

Pour une équation binôme de degré premier, on retrouve l'équivalence

irréductible $\Leftrightarrow$ sans racines

que l'on a montrée directement (voir p. 126).

- Le groupe de Galois de $X^3 - 2$ sur $\mathbb{Q}$ est Σ_3 , mais sur $\mathbb{Q}(j)$ c'est bien le groupe cyclique C_3 .
- Le corps $\mathbb{Q}(i)$ contient les racines quatrièmes de l'unité, $X^4 - 2$ est irréductible donc son groupe de Galois est cyclique d'ordre 4, engendré par

$$\sqrt[4]{2} \rightarrow i\sqrt[4]{2}$$

en notant $\sqrt[4]{2}$ la racine quatrième réelle positive de 2 (par exemple).

Par contre, sur $\mathbb{Q}$, le groupe de Galois est plus grand, il est d'ordre 8 car i peut avoir pour image i ou $-i$, et

$$(\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}) \rightarrow (\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}, i\sqrt[4]{2})$$

est un $\mathbb{Q}$ -automorphisme mais pas un $\mathbb{Q}(i)$ -automorphisme.

L'équation binôme de degré 4.

Si x est un rationnel non nul, nous allons étudier quel peut être le groupe de Galois du polynôme

$$P = X^4 - x$$

sur $\mathbb{Q}$.

D'abord quelques remarques :

- si u est une racine de P dans $\mathbb{C}$, les quatre racines sont

$$u, -u, iu, -iu,$$

et le corps de rupture est $\mathbb{Q}(u, i)$, de degré au plus égal à $4 \times 2 = 8$;

- l'ordre du groupe de Galois est au plus 8;

QUELQU

- si P

le corps $\mathbb{C}$
l'identité

- si P
factorisat
l'on vient

1° Cor
L'étude
d'une déc

dans $\mathbb{Q}[\sqrt[4]{2}]$

Reste à é

Si α es
décompos

Si α est

On en
carré et o

d'où

ce qui exi
pour la ré

Écrivor
n-ième da

- si P possède une racine dans $\mathbb{Q}$, soit v , alors $-v$ est aussi racine, et P est égal à

$$(X^2 - v^2)(X^2 + v^2);$$

le corps de rupture est alors $\mathbb{Q}(i)$ et le groupe de Galois est d'ordre 2, formé de l'identité et de la conjugaison complexe;

- si P est réductible sur $\mathbb{Q}$, il possède un facteur de degré 2 car, dans une factorisation propre $P = RS$, l'un des polynômes R ou S est de degré 2 ou 1 et l'on vient de voir que si P a un facteur de degré 1 il en a un de degré 2.

1° Conditions de réductibilité.

L'étude des conditions de réductibilité de P équivaut à l'étude de l'existence d'une décomposition :

$$X^4 - x = (X^2 + \alpha X + \beta)(X^2 + \alpha' X + \beta')$$

dans $\mathbb{Q}[X]$. On trouve tout de suite $\alpha + \alpha' = 0$ et $\beta\beta' = -x$, d'où

$$X^4 - x = (X^2 + \alpha X + \beta)\left(X^2 - \alpha X - \frac{x}{\beta}\right).$$

Reste à égaliser les coefficients de X^2 et X dans les deux membres, ce qui donne

$$\beta - \alpha^2 - \frac{x}{\beta} = 0$$

$$\alpha\beta + \frac{\alpha x}{\beta} = 0.$$

Si α est nul, il reste $\beta^2 = x$, et x possède une racine carrée dans K ; une décomposition est alors

$$X^4 - x = (X^2 + \beta)(X^2 - \beta).$$

Si α est non nul, les conditions s'écrivent

$$\begin{cases} \alpha^2\beta + x - \beta^2 = 0 \\ \beta^2 + x = 0. \end{cases}$$

On en déduit l'égalité $\alpha^2\beta + 2x = 0$; on l'écrit $\alpha^2\beta = -2x$, on l'élève au carré et on remplace β^2 par $-x$. On trouve alors

$$- \alpha^4 x = 4x^2$$

d'où

$$\alpha^4 = -4x$$

ce qui exige que $-4x$ possède une racine quatrième dans $\mathbb{Q}$. Et c'est suffisant pour la réductibilité de P , comme le montre la décomposition

$$X^4 - x = \left(X^2 + \alpha X + \frac{\alpha^2}{2}\right)\left(X^2 - \alpha X + \frac{\alpha^2}{2}\right).$$

Écrivons symboliquement « $\sqrt[n]{a} \in \mathbb{Q}$ » pour dire que a possède une racine n -ième dans $\mathbb{Q}$ (pas forcément toutes : la notation est dangereuse...).

On a alors montré

$$X^4 - x \text{ réductible sur } \mathbb{Q} \Leftrightarrow \sqrt{x} \in \mathbb{Q} \text{ ou } \sqrt[4]{-4x} \in \mathbb{Q}.$$

Bien entendu, on écrira aussi

$$X^4 - x \text{ possède un facteur de degré 1 sur } \mathbb{Q} \Leftrightarrow \sqrt[4]{x} \in \mathbb{Q}.$$

Faisons encore une remarque importante qui éclaire bien le rôle joué par $-4x$ dans l'étude du polynôme $X^4 - x$.

Cette remarque est la suivante : une racine quatrième de (-1) est $\frac{1+i}{\sqrt{2}}$, donc si l'on note $\sqrt[4]{y}$ une racine quatrième de y , alors une racine quatrième de $-y$ sera

$$\frac{1+i}{\sqrt{2}} \sqrt[4]{y} = \frac{1+i}{2} \sqrt[4]{4y}.$$

On passe donc d'une racine de $X^4 - 4y$ à une racine de $X^4 + y$ en multipliant par $\frac{1+i}{2}$, ce qui montre que, sur tout corps contenant i , les deux polynômes $X^4 - x$ et $X^4 + 4x$ ont même corps de rupture.

Or de toutes façons, le corps de rupture de chacun contient i .

Cette remarque permet de passer du cas $x > 0$ au cas $x < 0$.

2° Étude du cas $x > 0$.

Il y aura trois cas pour le polynôme $X^4 - x \in \mathbb{Q}[X]$ quand x est positif, suivant qu'il existe une racine, que le polynôme est réductible sans racine ou qu'il est irréductible. La circonstance $\sqrt[4]{-4x} \in \mathbb{Q}$ est ici à exclure, car $-4x$ est négatif.

• $\sqrt[4]{x} \in \mathbb{Q}$. Ici, $X^4 - x$ possède une racine rationnelle, donc deux, le corps de rupture est $\mathbb{Q}(i)$ et le groupe de Galois est d'ordre 2, formé de l'identité et la conjugaison complexe. On écrira $G(X^4 - x) = C_2$.

Un exemple : $X^4 - 16$, dont la décomposition en facteurs premiers sur $\mathbb{Q}$ est

$$(X - 2)(X + 2)(X^2 + 4)$$

alors que sur son corps de rupture $\mathbb{Q}(i)$ c'est

$$(X - 2)(X + 2)(X - 2i)(X + 2i).$$

Autre exemple : $X^4 - 1$, dont le corps de rupture $\mathbb{Q}(i)$ est le corps cyclotomique d'indice 4.

• $\sqrt{x} \in \mathbb{Q}$ et $\sqrt[4]{x} \notin \mathbb{Q}$. En appelant d la racine carrée positive de x dans $\mathbb{Q}$, la décomposition en facteurs premiers dans $\mathbb{Q}[X]$ est

$$X^4 - x = (X^2 - d)(X^2 + d).$$

Le corps de rupture est $\mathbb{Q}(\sqrt{d}, i)$, de degré 4 car $\sqrt{d}$ est de degré 2 sur $\mathbb{Q}$, et i est

de deg
 $C_2 \times C_2$
permut
l'identit
automo

Le se
Le gr
du poly

• $\sqrt{x}$
une de s
quatrième
minimum
rupture

Pour
racines.
transfor
Le pr
seconde.

Or un
est égale
écrivait

De pl

montren
engendr

Dans
éléments
générate
l'autre p
en $-i$

de degré 2 sur le corps réel $\mathbb{Q}(\sqrt{d})$. Le groupe de Galois est d'ordre 4, c'est $C_2 \times C_2$ (démonstration analogue au cas de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$) : les bonnes permutations de la suite des racines $(\sqrt{d}, -\sqrt{d}, i\sqrt{d}, -i\sqrt{d})$ sont, outre l'identité, les transpositions (1 2) et (3 4) et leur produit (1 2)(3 4), les trois automorphismes correspondants du corps de rupture $\mathbb{Q}(\sqrt{d}, i)$ étant

$$\begin{aligned}\lambda_0 + \lambda_1\sqrt{d} + \lambda_2i + \lambda_3i\sqrt{d} &\rightarrow \lambda_0 - \lambda_1\sqrt{d} + \lambda_2i - \lambda_3i\sqrt{d} \\ &\rightarrow \lambda_0 + \lambda_1\sqrt{d} - \lambda_2i - \lambda_3i\sqrt{d} \\ &\rightarrow \lambda_0 - \lambda_1\sqrt{d} - \lambda_2i + \lambda_3i\sqrt{d}.\end{aligned}$$

Le second est la conjugaison complexe.

Le groupe de Galois n'est pas transitif, ce qui est en accord avec la réductibilité du polynôme.

Un exemple : $X^4 - 4$, le réel $\sqrt{d}$ étant la racine carrée positive de 2.

• $\sqrt{x} \in \mathbb{Q}$. Le polynôme $X^4 - x$ est alors irréductible sur $\mathbb{Q}$, et si u désigne une de ses racines le corps de rupture est $\mathbb{Q}(u, i)$. On peut choisir pour u la racine quatrième réelle positive de x . En ce cas u est de degré 4 sur $\mathbb{Q}$ (son polynôme minimum est $X^4 - x$) et i de degré 2 sur le corps réel $\mathbb{Q}(u)$, donc le corps de rupture est de degré 8 sur $\mathbb{Q}$, et l'ordre du groupe de Galois $G(X^4 - x)$ est 8.

Pour le voir de plus près, appelons $(u, -u, iu, -iu)$ la famille des quatre racines. Il y a alors quatre automorphismes de $\mathbb{Q}(u, i)$ conservant i , et quatre qui transforment i en $-i$.

Le produit d'un de la première catégorie par un de la seconde est dans la seconde, donc la seconde catégorie engendre le groupe.

Or un automorphisme qui transforme i en $-i$ est donné par l'image de u , qui est égale à l'une des quatre racines. Faisons la liste de ces automorphismes, en écrivant la permutation qui lui correspond :

$$\begin{array}{lll}u \rightarrow u & (u, -u, iu, -iu) \rightarrow (u, -u, -iu, iu) & (3\ 4) \\u \rightarrow -u & (u, -u, iu, -iu) \rightarrow (-u, u, iu, -iu) & (1\ 2) \\u \rightarrow iu & (u, -u, iu, -iu) \rightarrow (iu, -iu, u, -u) & (1\ 3)(2\ 4) \\u \rightarrow -iu & (u, -u, iu, -iu) \rightarrow (-iu, iu, -u, u) & (1\ 4)(2\ 3).\end{array}$$

De plus, les deux égalités

$$\begin{aligned}(1\ 2)(1\ 3)(2\ 4)(1\ 2) &= (1\ 4)(2\ 3) \\(1\ 3)(2\ 4)(1\ 2)(1\ 3)(2\ 4) &= (3\ 4)\end{aligned}$$

montrent que la seconde, (1 2), et la troisième, (1 3)(2 4), suffisent pour engendrer le groupe. Toutes deux ont pour carré l'identité.

Dans ces conditions, le groupe $G(X^4 - x)$ est d'ordre 8 et engendré par deux éléments involutifs. C'est le groupe des isométries d'un carré, les deux générateurs correspondant à deux symétries, l'une par rapport à une diagonale et l'autre par rapport à une médiatrice. Les quatre automorphismes transformant i en $-i$ correspondent aux quatre symétries du carré (la première, (3 4), n'est

autre que la conjugaison complexe) alors que les quatre $\mathbb{Q}(i)$ -automorphismes forment le groupe des rotations ; par exemple, la rotation de π , ou symétrie par rapport au centre, est la seule permutation qui conserve i , ne conserve pas u et est involutive, c'est donc

$$(u, -u, iu, -iu) \rightarrow (-u, u, -iu, iu)$$

c'est-à-dire $(1\ 2)(3\ 4)$, produit des deux symétries $(1\ 2)$ et $(3\ 4)$.

On appelle groupe diédral d'ordre 8, et on note D_8 , le groupe des symétries du carré (voir *Le Défi algébrique*, tome I, page 310). On écrira donc, pour $x > 0$ et $\sqrt[4]{x} \notin \mathbb{Q}$, l'égalité : $G(X^4 - x) = D_8$.

L'exemple le plus usuel est celui de $X^4 - 2$. Un exemple de mauvaise permutation des racines est $(1\ 3)$, soit

$$(\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}) \rightarrow (i\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}, -i\sqrt[4]{2})$$

qui ne respecte pas la relation rationnelle $x_1 + x_2 = 0$. Avec cette numérotation, on écrira

$$(1\ 3) \notin G(X^4 - 2).$$

Par contre, la permutation $(1\ 3)(2\ 4)$ est une bonne permutation, elle correspond à l'automorphisme suivant du corps de rupture $\mathbb{Q}(\sqrt[4]{2}, i)$ (où les λ_i sont rationnels, et on a posé $u = \sqrt[4]{2}$, racine quatrième réelle positive de 2) :

$$\begin{aligned} \lambda_0 + \lambda_1 u + \lambda_2 u^2 + \lambda_3 u^3 + \lambda_4 i + \lambda_5 iu + \lambda_6 iu^2 + \lambda_7 iu^3 \\ \rightarrow \lambda_0 + \lambda_3 u - \lambda_2 u^2 - \lambda_7 u^3 - \lambda_4 i + \lambda_1 iu + \lambda_6 iu^2 - \lambda_5 iu^3. \end{aligned}$$

En effet, $i = \frac{iu}{u}$ a pour image $\frac{u}{iu} = \frac{1}{i} = -i$.

3° Étude du cas $x < 0$.

On a vu que le corps de rupture de $X^4 - x$ est le même que celui de $X^4 + 4x$ sur $\mathbb{Q}$.

Posons $y = -x$. On étudie donc le corps de rupture de $X^4 + y$ où y est positif, c'est celui de $X^4 - 4y$, d'où les trois cas, parmi lesquels seul le premier correspond à un polynôme $X^4 + y$ réductible.

• $\sqrt[4]{4y} \in \mathbb{Q}$, qui donne $G(X^4 + y) = C_2$. Le corps de rupture est $\mathbb{Q}(i)$: en appelant α la racine quatrième rationnelle positive de $4y$, la décomposition en facteurs premiers sur $\mathbb{Q}$ est

$$X^4 + y = \left(X^2 + \alpha X + \frac{\alpha^2}{2}\right) \left(X^2 - \alpha X + \frac{\alpha^2}{2}\right)$$

et les quatre racines sont

$$(\pm 1 \pm i) \frac{\alpha}{2}.$$

• $\sqrt{y} \in \mathbb{Q}$
correspond

Si l'on a
racines de $X^4 + y$
sont donc

ou encore

où z est la r

carré $\frac{\sqrt{y}}{2}$ ét

Le polyn

il n'y a que
étant z ou
(1 2)(3 4),
la conjugais
Le group

automorphismes
ou symétrie par
serve pas u et est

4).

des symétries du
ic, pour $x > 0$ et

Un exemple de
it

$\sqrt[4]{2}, -i\sqrt[4]{2}$
 $+ x_2 = 0$. Avec

nne permutation,
corps de rupture
é $u = \sqrt[4]{2}$, racine

$u^2 + \lambda_7 i u^3$
 $+ \lambda_6 i u^2 - \lambda_3 i u^3$.

celui de $X^4 - 4x$

$X^4 + y$ où y est
le seul le premier

ture est $\mathbb{Q}(i)$: en
décomposition en

$\begin{pmatrix} 2 \\ 1 \end{pmatrix}$

Un exemple : $X^4 + 4$, où α est égal à 2 et les quatre racines sont $\pm 1 \pm i$. Si on les écrit

$$(1 + i, 1 - i, -1 + i, -1 - i)$$

la seule bonne permutation autre que l'identité est $(1\ 2)(3\ 4)$, c'est la conjugaison complexe. La permutation $(1\ 2)$, par exemple, ne respecte pas la relation rationnelle $x_1 + x_4 = 0$. La décomposition en facteurs premiers s'écrit ici

$$X^4 + 4 = (X^2 + 2X + 2)(X^2 - 2X + 2).$$

• $\sqrt{y} \in \mathbb{Q}$ et $\sqrt[4]{4y} \notin \mathbb{Q}$ (la condition $\sqrt{4y} \in \mathbb{Q}$ équivaut en effet à $\sqrt{y} \in \mathbb{Q}$), qui correspond au groupe de Galois

$$G(X^2 + y) = C_2 \times C_2.$$

Si l'on appelle v la racine carrée réelle positive du rationnel positif $\sqrt{y}$, les racines de $X^4 + y$ sont les produits de v par les racines quatrièmes de -1 , ce sont donc

$$\frac{\pm 1 \pm i}{\sqrt{2}} v$$

ou encore

$$(\pm 1 \pm i)z$$

où z est la racine quatrième réelle positive de $\frac{y}{4}$; l'élément z est de degré 2, son carré $\frac{\sqrt{y}}{2}$ étant dans $\mathbb{Q}$.

Le polynôme $X^4 + y$ est irréductible sur $\mathbb{Q}$. Si l'on écrit la suite des racines

$$(1 + i)z, (-1 - i)z, (1 - i)z, (-1 + i)z,$$

il n'y a que quatre bonnes permutations, l'image de i étant i ou $-i$, et celle de z étant z ou $-z$. On trouve, outre l'identité, les trois permutations $(1\ 3)(2\ 4)$, $(1\ 2)(3\ 4)$, $(1\ 4)(2\ 3)$, la première étant la trace, sur le corps de rupture $\mathbb{Q}(z, i)$, de la conjugaison complexe.

Le groupe de Galois est transitif, comme il sied à un polynôme irréductible.

On peut prendre ici pour exemple le polynôme $X^4 + 1$, dont les racines sont $\frac{\pm 1 \pm i}{\sqrt{2}}$ et le corps de rupture est $\mathbb{Q}(\sqrt{2}, i)$. Ou

encore $X^4 + 9$, dont les racines sont $\frac{\pm 1 \pm i}{2} \sqrt{6}$ et le corps de rupture est $\mathbb{Q}(\sqrt{6}, i)$.

Avec les notations ci-dessus $\left(z = \frac{\sqrt{6}}{2}\right)$, la permutation

(1 2)(3 4) est bonne, elle transforme chaque racine en son opposée, mais ce n'est pas la transformation « opposition » du corps de rupture (qui n'est pas un automorphisme). C'est la transformation

$$\lambda_0 + \lambda_1 i + \lambda_2 \sqrt{6} + \lambda_3 i \sqrt{6} \rightarrow \lambda_0 + \lambda_1 i - \lambda_2 \sqrt{6} - \lambda_3 i \sqrt{6}.$$

• $\sqrt{y} \notin \mathbb{Q}$. Le polynôme $X^4 + y$ est toujours irréductible, mais son groupe de Galois est d'ordre 8, c'est le groupe diédral D_8 .

Le corps de rupture de $X^4 + y$ est $\mathbb{Q}(\sqrt[4]{4y}, i)$, en appelant $v = \sqrt[4]{4y}$ la racine quatrième réelle positive de $4y$. Les quatre racines s'écrivent

$$\frac{1+i}{2}v, \frac{-1-i}{2}v, \frac{1-i}{2}v, \frac{-1+i}{2}v,$$

et les huit bonnes permutations correspondent à la transformation de i en i ou $-i$, et de v en $v, -v, iv$, ou $-iv$ (alors que $v \rightarrow \pm iv$ étaient mauvaises dans le cas précédent).

L'exemple le plus simple est ici $X^4 + 2$, dont les racines sont

$$\frac{\pm 1 \pm i}{\sqrt[4]{2}}$$

et le corps de rupture est

$$\mathbb{Q}(\sqrt[4]{8}, i) = \mathbb{Q}(\sqrt[4]{2}, i).$$

4° *Récapitulons* : pour un rationnel $r > 0$, écrivons les différents groupes de Galois G de $X^4 - r$ et $X^4 + r$ sur $\mathbb{Q}$.

• $X^4 - r$:

$$\begin{aligned} \sqrt[4]{r} \in \mathbb{Q} &\Rightarrow G = C_2 \\ \sqrt{r} \in \mathbb{Q} \text{ et } \sqrt[4]{r} \notin \mathbb{Q} &\Rightarrow G = C_2 \times C_2 \\ \sqrt{r} \notin \mathbb{Q} &\Rightarrow G = D_8 \end{aligned}$$

• $X^4 + r$:

$$\begin{aligned} \sqrt[4]{4r} \in \mathbb{Q} &\Rightarrow G = C_2 \\ \sqrt{r} \in \mathbb{Q} \text{ et } \sqrt[4]{4r} \notin \mathbb{Q} &\Rightarrow G = C_2 \times C_2 \\ \sqrt{r} \notin \mathbb{Q} &\Rightarrow G = D_8 \end{aligned}$$

Sur ces six cas, les premier, deuxième et quatrième correspondent à des polynômes réductibles, les trois autres à des polynômes irréductibles.

Une remarque : plongés dans Σ_4 , les deux sous-groupes de la liste isomorphes à $C_2 \times C_2$ sont en fait très différents.

Le premier est non transitif, c'est

$$\text{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)$$

le second, 1

il est transi
Et heure
irréductible

Exercices.

1. Étudie
pour

2. Décri
4, 6, 8

3. Comp
et de

4. Le no

est élé
Galois
group

5. Si H_1

6. On su
Galois
Étudi

sur $\mathbb{Q}$.

aque racine en son
on « opposition » du
morphisme). C'est la

$$- \lambda_2 \sqrt{6} - \lambda_3 i \sqrt{6}.$$

z, mais son groupe de

nt $v = \sqrt[4]{4y}$ la racine
ent

v,

nsformation de i en i
ient mauvaises dans le

ont les racines sont

s différents groupes de

correspondent à des
irréductibles.

de la liste isomorphes

le second, lui, est

$$\text{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$$

il est transitif.

Et heureusement... car $X^4 - r$ est réductible dans le premier cas, $X^4 + r$ irréductible dans le second.

Exercices.

1. Étudier le groupe de Galois de $X^4 - 5$ sur différents sous-corps de $\mathbb{C}$. De même pour $X^3 - 2$, pour $X^3 + 2X + 1$.
2. Décrire explicitement les groupes de Galois des corps cyclotomiques d'indices 4, 6, 8, 9.
3. Comparer le groupe de Galois de $X^{nm} - 1$ sur $\mathbb{Q}$ aux groupes de Galois de $X^n - 1$ et de $X^m - 1$.
4. Le nombre complexe

$$z = e^{\frac{2i\pi}{17}}$$

est élément primitif du corps de rupture de $X^{17} - 1$. Montrer que le groupe de Galois est engendré par l'automorphisme $z \rightarrow z^3$ (on vérifiera que 3 engendre le groupe multiplicatif $\mathbb{Z}/17\mathbb{Z}$).

5. Si H_1 et H_2 sont des corps intermédiaires entre K et L , montrer

$$G(L|H_1 H_2) = G(L|H_1) \cap G(L|H_2).$$

6. On suppose que $P(X)$ divise $P(X^2 - 2)$ dans $K[X]$. Que peut-on dire du groupe de Galois de P sur K ? Étudier les cas

$$P = X^3 - 3X + 1,$$

$$P = X^3 + X^2 - 2X - 1$$

sur $\mathbb{Q}$.

Les conjugués d'un élément algébrique

On a déjà signalé deux fois au passage le mot « conjugué ». Dans l'étude d'une équation, on avait appelé conjugués d'un élément qui s'exprimait à l'aide des racines tous les éléments qui s'écrivaient de la même manière à des permutations près des racines (voir p. 49). On a aussi parlé de conjugués d'un élément d'une extension comme des racines de son polynôme minimum (voir p. 96).

Il est temps de préciser ces notions un peu vagues.

Les conjugués d'un élément par rapport à un polynôme.

Partons encore d'un polynôme $P \in K[X]$, et appelons $(x_1, \dots, x_n)$ ses racines, son corps de rupture sur K étant alors

$$L = K(x_1, \dots, x_n).$$

Un élément de ce corps de rupture s'écrit

$$z = T(x_1, \dots, x_n)$$

pour un certain polynôme $T \in K[X_1, \dots, X_n]$ et, si l'on effectue une permutation σ des indices, on a vu que l'on ne peut pas toujours, à partir de z , définir un élément $\sigma z = T(x_{\sigma(1)}, \dots, x_{\sigma(n)})$: en effet, le T correspondant à z n'est pas unique. C'était là notre distinction entre les bonnes et mauvaises permutations (voir p. 135).

Si σ est une *bonne* permutation, c'est-à-dire appartient au groupe de Galois de P sur K , alors σz est bien défini, car $T(x_{\sigma(1)}, \dots, x_{\sigma(n)})$ dépend seulement de z et pas du T choisi pour le représenter. Ces éléments σz ainsi obtenus quand σ décrit le groupe de Galois $G(P)$ s'appellent les **conjugués** de z par rapport au polynôme P . Bien entendu, cette relation de conjugaison est une relation d'équivalence dans le corps de rupture L .

On peut les voir d'une autre manière, vu la correspondance naturelle entre les bonnes permutations des racines et les K -automorphismes du corps de rupture L de P sur K . Ces conjugués de $z \in L$ sont alors ses images par tous les K -automorphismes de L , ce qui montre qu'ils ne dépendent que du corps de rupture : si deux polynômes ont même corps de rupture, la notion de conjugué est la même par rapport aux deux. C'est pourquoi un K -automorphisme d'un corps de rupture s'appelle souvent une **conjugaison** de ce corps de rupture et, au lieu de dire que deux éléments sont conjugués par rapport au polynôme, on peut dire qu'ils le sont par rapport au corps de rupture.

On peut donc, pour calculer les conjugués de $z \in L$, où L est corps de rupture de P sur K :

- soit prendre les images de z par tous les K -automorphismes de L ;
- soit écrire z en fonction rationnelle des racines de P et appliquer à cette fonction toutes les bonnes permutations des racines.

Dans le premier cas on est plus « axé » sur le corps de rupture, dans le second cas c'est le polynôme lui-même qui nous intéresse plus.

Algébrique

Dans l'étude d'une racine primitive ζ_n on s'intéresse à l'aide des racines de l'unité et des permutations de ces racines (voir p. 96).

..., x_n) ses racines.

Si on a une permutation σ de $\{1, \dots, n\}$, on définit un automorphisme σ de L en posant $\sigma(x_i) = x_{\sigma(i)}$. On vérifie que σ est une permutation de L et que $\sigma^2 = \text{id}$. On appelle σ la conjugaison de L par abus de langage.

Le groupe de Galois de L/K est d'ordre 2 et est engendré par σ . On appelle σ la conjugaison de L par abus de langage.

La conjugaison de L par σ est la seule permutation non triviale de L qui fixe K . On appelle σ la conjugaison de L par abus de langage.

• Le premier exemple est celui de $\mathbb{C}$, corps de rupture de $X^2 + 1$ sur $\mathbb{R}$ (ou de tout polynôme réel à discriminant strictement négatif). Les seuls $\mathbb{R}$ -automorphismes de $\mathbb{C}$ sont l'identité et la conjugaison complexe (qui échange les racines i et $-i$). Heureusement, cette conjugaison complexe est bien une... conjugaison au sens ci-dessus !

• Plus généralement, pour une extension quadratique L de K , il y a une seule conjugaison autre que l'identité, c'est celle que l'on appelle la conjugaison de L par abus de langage.

Pour la définir, on prend un élément x de L ayant une racine carrée dans L et pas dans K : alors tout élément de $L = K(\sqrt{x})$ s'écrit de manière unique $a + b\sqrt{x}$, où $\sqrt{x}$ est une racine carrée choisie de x dans L , et la conjugaison de L est

$$a + b\sqrt{x} \rightarrow a - b\sqrt{x}$$

indépendante du choix de x (par exemple $4x$ convient aussi). Un tel x est, par exemple, le discriminant du polynôme minimum (de degré 2) d'un élément arbitraire de $L \setminus K$.

• Prenons $x = \frac{1+i}{\sqrt{2}}$, racine complexe de i . Cet élément est à la fois dans le corps de rupture de $X^4 + 1$ sur $\mathbb{Q}$, dans celui de $X^2 - 2$ sur $\mathbb{Q}(i)$, et dans celui de $X^2 + 1$ sur $\mathbb{Q}(\sqrt{2})$ ou sur $\mathbb{R}$.

Dans le premier contexte, il a quatre conjugués, qui sont $\pm \frac{1 \pm i}{\sqrt{2}}$, les quatre racines de son polynôme minimum $X^4 + 1$.

Dans le second contexte, la seule bonne permutation autre que l'identité est l'échange de $\sqrt{2}$ et $-\sqrt{2}$, donc les conjugués de x sont x et $-x$; ce sont les racines du polynôme minimum $X^2 - i$ de x sur $\mathbb{Q}(i)$.

Enfin, dans le troisième cas, les seuls automorphismes du corps de rupture conservant le corps de base sont l'identité et la conjugaison complexe, donc les conjugués de x sont x et $\bar{x}$ qui se trouvent bien sûr être les racines du polynôme minimum $X^2 - X\sqrt{2} + 1$ de x sur $\mathbb{Q}(\sqrt{2})$ ou sur $\mathbb{R}$.

Les conjugués comme racines du polynôme minimum.

Comme on l'a signalé, la notion de conjugués d'un élément z du corps de rupture de $P \in K[X]$ sur K a été d'abord définie à partir des racines $(x_1, \dots, x_n)$ de P : l'élément z s'écrit comme valeur en $(x_1, \dots, x_n)$ d'un certain polynôme $T \in K[X_1, \dots, X_n]$, et ses conjugués forment la *famille*

$$(T(x_{\sigma(1)}, \dots, x_{\sigma(n)}))_{\sigma \in G(P)}.$$

Le fait de se réduire à $G(P)$ au lieu de Σ_n assure que les conjugués ne dépendent pas du choix du polynôme T .

En une seconde étape, on a montré que cette famille ne dépendait de P que par l'intermédiaire de son corps de rupture L , car c'est aussi la famille

$$(\varphi(z))_{\varphi \in G(L)}$$

φ décrivant le groupe $G(L)$ des K -automorphismes de L .

En une troisième étape, on va montrer qu'en un certain sens même le corps L est superflu : si on le remplace par un *autre* corps de rupture contenant x , l'ensemble des conjugués sera le même. Autrement dit, les conjugués de x sur K ne dépendent que de x et de K , non du corps de rupture dans lequel on place $K(x)$: le corps de rupture le plus « simple » sera alors celui du polynôme minimum de x sur K .

Plus précisément, on va montrer le résultat suivant (vérifié sur les exemples ci-dessus) :

Les conjugués d'un élément sur un corps sont les racines de son polynôme minimum.

Dans un sens, c'est facile : le polynôme minimum de x sur K est fixe par tout K -automorphisme, donc toute image de x en est encore racine.

La réciproque est un peu plus difficile. On part de K et d'un élément α d'un corps de rupture L sur K . Si M_α est le polynôme minimum de α sur K , et si β est une racine de M_α dans une extension de K , deux questions se posent :

- β est-il dans L aussi ?
- Existe-t-il un K -automorphisme de L transformant α en β ?

La première question s'énonce : si un corps de rupture contient une racine d'un polynôme irréductible sur le corps de base, le contient-ils toutes ?

Comme α et β ont même polynôme minimum sur K , on a montré que l'on peut définir la « substitution de α par β » : si R_1 et R_2 sont des polynômes sur K ayant même valeur en α , ils ont même valeur en β car leur différence est multiple du polynôme minimum commun.

D'où l'isomorphisme de corps $(R$ décrivant l'ensemble des polynômes sur $K)$

$$\psi : R(\alpha) \rightarrow R(\beta)$$

$$K(\alpha) \rightarrow K(\beta)$$

laissant K fixe : c'est un K -isomorphisme de corps.

Mais L
($a_1, \dots, a_n$)
un K -isom
de Q sur L

le second e
les racines
 β appartient
donc β et

Pour pr

en

on remarque
de Q , donc
Sinon, on p
minimum s
racine b_1 (o
en déduit u

qui transfor
fixe par ψ_1 ;
de degrés e

on recomm
alors le K -

Une parent

On a dé
réductible r
deux élém
l'un en l'au
Les résul

En effet,
vient de
un K -autor
termes, que

Mais L est corps de rupture sur K d'un polynôme $Q \in K[X]$, de racines $(a_1, \dots, a_n)$. Par adjonctions successives des racines de Q , on va prolonger ψ en un K -isomorphisme $\bar{\psi}$ du corps de rupture de Q sur $K(\alpha)$ dans le corps de rupture de Q sur $K(\beta)$. Le premier corps de rupture est

$$K(\alpha, a_1, \dots, a_n) = K(a_1, \dots, a_n) = L$$

le second est $K(\beta, a_1, \dots, a_n)$, qui sera égal aussi à L grâce au fait que $\bar{\psi}$ permute les racines de Q ; α , donc aussi son image β , est un polynôme en ces racines, donc β appartient à $K(a_1, \dots, a_n) = L$. Dès lors, $\bar{\psi}$ sera un K -automorphisme de L , donc β et α seront bien conjugués dans L sur K .

Pour prolonger

$$\psi : K(\alpha) \rightarrow K(\beta)$$

en

$$\bar{\psi} : K(\alpha, a_1, \dots, a_n) \rightarrow K(\beta, a_1, \dots, a_n)$$

on remarque d'abord que, si l'un des a_i est dans $K(\alpha)$, son image $\psi(a_i)$ est racine de Q , donc un des a_j . Le problème est donc réglé si tous les a_i sont dans $K(\alpha)$. Sinon, on procède pas à pas en prenant par exemple $a_1 \notin K(\alpha)$; son polynôme minimum sur $K(\alpha)$ est de degré supérieur à 2, donc l'image de ce polynôme a une racine b_1 (on peut se placer dès le départ dans une clôture algébrique de K) et on en déduit un K -isomorphisme

$$\psi_1 : K(\alpha, a_1) \rightarrow K(\beta, b_1)$$

qui transforme a_1 en b_1 . Mais l'égalité $Q(a_1) = 0$ entraîne $Q(b_1) = 0$, car Q est fixe par ψ_1 ; dans ces conditions b_1 est l'un des a_i , soit a_{i_1} , hors de $K(\alpha)$ pour raison de degrés et, à partir du K -isomorphisme

$$\psi_1 : K(\alpha, a_1) \rightarrow K(\beta, a_{i_1})$$

on recommence jusqu'à arriver au corps de rupture L de Q sur K : on trouve alors le K -automorphisme $\bar{\psi}$ de L cherché.

Une parenthèse : les groupes de Galois transitifs.

On a déjà montré (voir p. 142) que le groupe de Galois d'un polynôme réductible n'était pas transitif sur la famille des racines du polynôme : il existe deux éléments de cette famille tels qu'aucune bonne permutation ne transforme l'un en l'autre.

Les résultats précédents permettent de montrer la réciproque.

Le groupe de Galois d'un polynôme irréductible est transitif.

En effet, si α et β sont deux racines d'un polynôme P irréductible sur K , on vient de voir que α et β sont conjugués sur K , donc qu'il existe un K -automorphisme du corps de rupture transformant α en β . En d'autres termes, quels que soient α et β racines de P , il existe $\sigma \in G(P)$ avec $\sigma(\alpha) = \beta$.

On voit où intervient l'irréductibilité de P : c'est elle qui permet d'assurer que α et β sont conjugués sur K .

En n'oubliant pas que, dans le cas d'un polynôme primaire (puissance d'un irréductible), il convient de considérer la famille des racines (donc de répéter les racines multiples éventuelles), on dira de manière concise :

polynôme irréductible $\Leftrightarrow$ groupe de Galois transitif.

Les groupes de Galois sur des corps finis.

Une application simple : si P est un polynôme sur le corps fini K , son groupe de Galois est un sous-groupe du groupe cyclique des automorphismes du corps de rupture de P (voir p. 143), il est donc aussi cyclique. Or le groupe cyclique engendré par $\sigma \in \Sigma_n$ est transitif si, et seulement si, σ est un cycle de longueur n , car sinon on prend i et j dans deux composantes cycliques de σ et aucune puissance de σ ne transformera i en j . D'où l'équivalence, pour P de degré n sur le corps fini K et sans racine double :

P irréductible sur $K \Leftrightarrow G(P|K)$ engendré par un cycle de longueur n .

Si P est arbitraire sur le corps fini K (mais toujours sans racine double), on le décompose en facteurs premiers dans $K[X]$

$$P = P_1 \dots P_m.$$

Le groupe de Galois $G(P|K)$ est engendré par une permutation σ que l'on décompose en produit de cycles disjoints : $\sigma = \sigma_1 \dots \sigma_r$.

Comme σ laisse stable l'ensemble des racines de P_1 et que la restriction de σ à cet ensemble doit engendrer un sous-groupe transitif sur ces racines, cette restriction est un cycle et c'est l'un des σ_i .

On en déduit que σ_1 a pour longueur le degré de l'un des P_i , σ_2 celui d'un autre, etc.

En conclusion, le groupe de Galois de P sur K est engendré par un produit de cycles dont les longueurs respectives sont les degrés des facteurs irréductibles de P .

Exemple : sur $\mathbb{Z}/5$, on écrit

$$X^5 + 2X^2 + X + 4 = (X^2 + 2)(X^3 + 3X + 2).$$

Les deux facteurs du second membre sont irréductibles, donc le groupe de Galois de

$$X^5 + 2X^2 + X + 4$$

sur $\mathbb{Z}/5$ est, après un numérotage adéquat des racines, engendré par $(1, 2)(3, 4, 5)$.

Une autre parenthèse : le groupe de Galois d'un facteur.

Soit, dans $K[X]$, un polynôme P divisant un polynôme T . Que peut-on dire des groupes de Galois de ces deux polynômes sur K ?

Si l'on
Mais les r
racine x de
En term
homomor

où σ' est l

Tout cel
demande
de démor
K-autom
pas », com
est aussi le
K-autom
racines de
En conc

Le noyau
Galois de

Une remar

La notio
laquelle on
En effet,
degré de L
longueur n
K-automoi
Mais ces
indépendan
l'ensemble

assurer que α
puissance d'un
de répéter les

f.

son groupe de
es du corps de
cyclique engen-
deur n , car
une puissance
 n sur le corps

ongueur n .

double), on le

ion σ que l'on

striction de σ à
racines, cette

, σ_2 celui d'un

par un produit
rs irréductibles

+ 2).

ctibles, donc le

sines, engendré

ue peut-on dire

Si l'on part d'un élément $\sigma \in G(T)$, c'est une permutation des racines de T . Mais les racines de P sont des racines particulières de T et l'image par σ d'une racine x de P est encore racine de P (car $P(x) = 0$ est une relation rationnelle sur K).

En termes plus savants, l'application « restriction aux racines de P » est un homomorphisme de $G(T)$ dans $G(P)$:

$$\begin{aligned}\sigma &\rightarrow \sigma' \\ G(T) &\rightarrow G(P)\end{aligned}$$

où σ' est la restriction de σ aux racines de P .

Tout cela est élémentaire. Par contre, le fait que cette application est surjective demande un résultat de « prolongement », celui que l'on vient précisément de démontrer : si l'on part de $s \in G(P)$, on le considère comme un K -automorphisme du corps de rupture K_1 de P sur K , et on le prolonge « pas à pas », comme on vient de le faire, au corps de rupture de K_2 de T sur K_1 ; mais K_2 est aussi le corps de rupture de T sur K , on trouve donc comme prolongement un K -automorphisme de K_2 , donc un élément de $G(T)$, dont s est la restriction aux racines de P .

En conclusion, $G(P)$ est l'image de $G(T)$ par un homomorphisme de groupe.

Le groupe de Galois d'un facteur d'un polynôme est un quotient du groupe de Galois de ce polynôme.

Le noyau est formé des K_1 -automorphismes de K_2 , c'est-à-dire du groupe de Galois de T sur le corps de rupture de P .

Ainsi, on trouve $G(X^2 - 2) = C_2$, qui est bien le quotient de

$$G((X^2 - 2)(X^2 - 3)) = C_2 \times C_2$$

par le groupe de Galois C_2 de $(X^2 - 2)(X^2 - 3)$ sur $\mathbb{Q}(\sqrt{2})$.

Une remarque.

La notion d'« élément conjugué de z » ne dépend pas de l'extension de K dans laquelle on se place, mais la *famille* des conjugués de z en dépend.

En effet, si l'on place z dans le corps de rupture L d'un polynôme et si m est le degré de L sur K , alors la famille des conjugués de z sur K par rapport à L est de longueur m , c'est la suite $(\varphi_1(z), \dots, \varphi_m(z))$ où les φ_i décrivent le groupe des K -automorphismes du corps de rupture L .

Mais ces éléments peuvent se répéter, le nombre de $\varphi_i(z)$ distincts étant, lui, indépendant de L : c'est le degré de z sur K , car l'ensemble $\{\varphi_1(z), \dots, \varphi_m(z)\}$ est l'ensemble des racines du polynôme minimum de z sur K .

Le cas caricatural est celui où z est dans K . Il est son seul conjugué, mais la famille de ses conjugués dans un corps de rupture de degré m est $(z, z, \dots, z)$, suite de longueur m .

Le calcul du polynôme minimum.

Dans ces conditions, si l'on considère l'ensemble des conjugués $\{\alpha_1, \alpha_2, \dots, \alpha_m\}$ de α sur K , le polynôme minimum de α sur K sera

$$\prod_{i=1}^m (X - \alpha_i).$$

Ce polynôme est forcément à coefficients dans K et irréductible sur K . On peut ainsi affirmer :

- les fonctions symétriques des conjugués d'un élément sont dans le corps de base ;
- le degré d'un élément algébrique est le nombre de ses conjugués.

En pratique, si α est exprimé à l'aide des racines du polynôme, soit $\alpha = \varphi(a_1, \dots, a_n)$, on écrit les $\varphi(a_{\sigma(1)}, \dots, a_{\sigma(n)})$ quand σ décrit le groupe de Galois, on prend une fois et une seule chaque valeur obtenue (ce sont les conjugués de α sur K), et le polynôme minimum de α est $\prod (X - u)$ quand u décrit l'ensemble de ces valeurs. Aucune vérification n'est nécessaire, en particulier en ce qui concerne l'irréductibilité.

Quelques exemples.

- Ainsi, si a, b, c sont les racines du polynôme $X^3 + pX + q$ supposé irréductible sur K (contenant $\mathbb{Q}$), les conjugués de a sont a, b, c et son polynôme minimum est (heureusement) :

$$(X - a)(X - b)(X - c) = X^3 + pX + q.$$

Le groupe de Galois est, on l'a vu, soit A_3 soit Σ_3 , suivant que $-4p^3 - 27q^2$ est ou n'est pas un carré dans K . Dans les deux cas, les conjugués de la somme $a + b$ de deux racines sont $a + b, a + c, b + c$, donc cette somme est de degré 3 et de polynôme minimum

$$(X - a - b)(X - a - c)(X - b - c)$$

que l'on peut aussi calculer à l'aide des fonctions symétriques élémentaires.

Quant à la différence $a - b$, elle aura seulement trois conjugués si le groupe de Galois est A_3 , ce seront $a - b, b - c, c - a$, alors qu'elle en aura six si ce groupe est Σ_3 : les trois ci-dessus et leurs opposés.

En d'autres termes, le polynôme minimum de $a - b$ sera de degré 3, égal à

$$(X - a + b)(X - b + c)(X - c + a)$$

si le groupe de Galois est A_3 (c'est-à-dire si les transpositions ne respectent pas les relations rationnelles sur K entre les racines), alors que le polynôme minimum de $a - b$ sera égal à

$$(X^2 - (a - b)^2)(X^2 - (b - c)^2)(X^2 - (a - c)^2)$$

dans le cas où le groupe de Galois est Σ_3 entier.

• On a vu que le groupe de Galois de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, corps de rupture de

$$(X^2 - 2)(X^2 - 3)$$

sur $\mathbb{Q}$, est produit de deux groupes d'ordre 2, engendrés par

$$\begin{array}{ccc} \sqrt{2} \rightarrow -\sqrt{2} & & \sqrt{2} \rightarrow \sqrt{2} \\ \sqrt{3} \rightarrow \sqrt{3} & \text{et} & \sqrt{3} \rightarrow -\sqrt{3}. \end{array}$$

Par suite, l'élément $\sqrt{2} + \sqrt{3}$ aura pour conjugués

$$\sqrt{2} + \sqrt{3}, \quad -\sqrt{2} + \sqrt{3}, \quad \sqrt{2} - \sqrt{3} \quad \text{et} \quad -\sqrt{2} - \sqrt{3}.$$

Il sera de degré 4, donc primitif, et de polynôme minimum :

$$\begin{aligned} (X^2 - (\sqrt{2} + \sqrt{3})^2)(X^2 - (\sqrt{2} - \sqrt{3})^2) \\ = (X^2 - 5 - 2\sqrt{6})(X^2 - 5 + 2\sqrt{6}) \\ = (X^2 - 5)^2 - 24 = X^4 - 10X^2 + 1. \end{aligned}$$

C'est bien le polynôme que l'on avait calculé directement et il est superflu de vérifier qu'il est irréductible sur $\mathbb{Q}$: tout polynôme sur $\mathbb{Q}$ s'annulant en $\sqrt{2} + \sqrt{3}$ doit s'annuler sur les quatre conjugués, donc être multiple de

$$X^4 - 10X^2 + 1.$$

• Soit x la racine cubique réelle de $1 - \sqrt{2}$. Le polynôme minimum de x sur $\mathbb{Q}$ est

$$X^6 - 2X^3 - 1$$

dont le corps de rupture est $\mathbb{Q}(x, j)$, de degré 12 (voir p. 121).

Dans ce corps, prenons $y = x + \sqrt{2}$, soit $y = \sqrt[3]{1 - \sqrt{2}} + \sqrt{2}$, ou encore $y = -x^3 + x + 1$. Comme le corps de rupture est de degré 2 sur $\mathbb{Q}(y) = \mathbb{Q}(x)$, la suite des douze conjugués de y par rapport à $X^6 - 2X^3 - 1$ sera formée de six éléments répétés deux fois chacun.

Pour les calculer, on applique à y les douze éléments du groupe de Galois. L'image de x est l'un des six éléments

$$x, \quad jx, \quad j^2x, \quad -\frac{1}{x} = \sqrt[3]{1 + \sqrt{2}}, \quad -\frac{j}{x}, \quad -\frac{j^2}{x},$$

et l'élément $\sqrt{2}$ est conservé dans les trois premiers cas, transformé en $-\sqrt{2}$ dans les trois seconds cas (car $\sqrt{2}$ est égal à $1 - x^3$). Il reste, comme conjugués de y , les six valeurs

$$y_1 = \sqrt[3]{1 - \sqrt{2}} + \sqrt{2}$$

$$y_2 = j\sqrt[3]{1 - \sqrt{2}} + \sqrt{2}$$

$$y_3 = j^2\sqrt[3]{1 - \sqrt{2}} + \sqrt{2}$$

$$y_4 = \sqrt[3]{1 + \sqrt{2}} - \sqrt{2}$$

$$y_5 = j\sqrt[3]{1 + \sqrt{2}} - \sqrt{2}$$

$$y_6 = j^2\sqrt[3]{1 + \sqrt{2}} - \sqrt{2}.$$

Le polynôme $\prod_{i=1}^6 (X - y_i)$ est nécessairement à coefficients rationnels et irréductible, c'est le polynôme minimum de y sur $\mathbb{Q}$. On trouve

$$X^6 - 6X^4 - 2X^3 + 24X^2 - 12X - 1.$$

On aurait aussi pu calculer ce polynôme minimum en écrivant

$$(y - \sqrt{2})^3 = 1 - \sqrt{2},$$

en isolant $\sqrt{2}$ et en élevant au carré.

• Dans le même exemple si, au lieu de $y = x + \sqrt{2}$, on prend $z = x + \sqrt{-3}$ qui est encore dans le corps de rupture $\mathbb{Q}(x, j)$, on trouve cette fois douze valeurs distinctes par le groupe de Galois : ce sont les douze valeurs obtenues en remplaçant x par l'un de ses six conjugués et $\sqrt{-3}$ par $\sqrt{-3}$ ou $-\sqrt{-3}$. La différence est que, ici, on remplace *indépendamment* les deux termes x et $\sqrt{-3}$ par des conjugués, alors que ci-dessus le choix du conjugué de x imposait l'image de $\sqrt{2}$.

Dès lors,

$$z = \sqrt[3]{1 - \sqrt{2}} + \sqrt{-3}$$

est élément primitif du corps de rupture du polynôme minimum de $x = \sqrt[3]{1 - \sqrt{2}}$ sur $\mathbb{Q}$, puisque son degré est le degré de ce corps sur $\mathbb{Q}$.

Une ap

Une
corps d

En su
du corp
élément
qui équ
distinct

Ainsi,
la fonct
la suite

est form
distinct
de fois.

A ce p
l'élémen

ois premiers cas,
 (car $\sqrt{2}$ est égal à
 six valeurs

Une application aux éléments primitifs.

Une importante conséquence est la détermination des éléments primitifs d'un corps de rupture; le dernier exemple ci-dessus montre la méthode.

En supposant toujours que K est un corps contenant $\mathbb{Q}$, les éléments primitifs du corps de rupture du polynôme $P \in K[X]$ sur K seront exactement les éléments dont le nombre de conjugués est égal au degré du corps de rupture, ce qui équivaut à dire que les images par le groupe de Galois sont deux à deux distinctes.

Ainsi, si $a_1, \dots, a_n$ sont les racines de P et si G est le groupe de Galois de P sur K , la fonction rationnelle $\varphi(a_1, \dots, a_n)$ des racines sera primitive si, et seulement si, la suite

$$(\varphi(a_{\sigma(1)}, \dots, a_{\sigma(n)}))_{\sigma \in G}$$

est formée d'éléments distincts. Dans le cas contraire, le nombre d'éléments distincts dans cette suite est un diviseur de n , car tous se répètent un nombre égal de fois.

- Ainsi, reprenons le polynôme irréductible

$$X^3 + pX + q \in K[X].$$

La somme de deux racines a trois conjugués distincts, donc sera primitive si, et seulement si, le groupe de Galois est A_3 , ce qui signifie

$$\sqrt{-4p^3 - 27q^2} \in K.$$

D'ailleurs, la somme de deux racines est égale à l'opposé de la troisième et chaque racine a trois conjugués. Une racine sera donc primitive sous la même condition (et alors bien sûr chacune l'est).

Quant à la différence de deux racines, elle a trois conjugués si le groupe est A_3 , six si le groupe est Σ_3 : dans tous les cas elle est primitive.

On l'a déjà vu en faisant le calcul explicite (voir p. 103).

- Pour $X^4 + 1$, le corps de rupture est $\mathbb{Q}(\sqrt{2}, i)$, de degré 4, et $i + \sqrt{2}$ possède quatre conjugués distincts: il est primitif.

- Le groupe de Galois de $X^4 + 2$ sur $\mathbb{Q}$ est d'ordre 8, le corps de rupture est $\mathbb{Q}(\sqrt[4]{2}, i)$ et les bonnes permutations sont celles qui transforment i en i ou $-i$, et $\sqrt[4]{2}$ en son produit par 1, -1 , i , ou $-i$. Dans ces conditions, $i + \sqrt[4]{2}$ possède huit conjugués distincts, il est donc primitif.

A ce point, un retour en arrière s'impose sur la démonstration du théorème de l'élément primitif dans le cas d'un corps de rupture (voir p. 104).

Si P est un polynôme sur K , de racines $(x_1, \dots, x_n)$, on a montré que la fonction rationnelle $F(x_1, \dots, x_n)$ est élément primitif dès qu'elle vérifie

$$\sigma \in \Sigma_n \setminus \text{id} \Rightarrow F(x_{\sigma(1)}, \dots, x_{\sigma(n)}) \neq F(x_1, \dots, x_n).$$

Cette condition était *suffisante*, mais non nécessaire.

Ainsi, $\sqrt{2} + \sqrt{3}$ est primitif pour le corps de rupture de

$$(X^2 - 2)(X^2 - 3)$$

sur $\mathbb{Q}$, mais la permutation qui échange $-\sqrt{2}$ et $-\sqrt{3}$ ne le change pas. Seulement voilà : ce n'est pas une bonne permutation, elle n'est pas dans le groupe de Galois.

La condition *nécessaire et suffisante* s'obtient en faisant décrire à σ , non pas tout le groupe Σ_n , mais seulement le groupe de Galois $G(P)$, c'est-à-dire en ne prenant pour σ que les bonnes permutations

$F(x_1, \dots, x_n)$ primitif $\Leftrightarrow F(x_1, \dots, x_n) \neq F(x_{\sigma(1)}, \dots, x_{\sigma(n)})$ pour tout $\sigma \in G(P) \setminus \text{id}$.

Cette condition est plus faible. Mais, en l'absence de la théorie de Galois, ou de la connaissance du groupe de Galois, on est sûr de tomber sur un élément primitif en remplaçant $G(P)$ par Σ_n tout entier.

Une importante caractérisation du corps de base.

Restons en caractéristique nulle. Alors, dans la clôture algébrique de K , la relation d'équivalence

« x et y sont conjugués sur K »

signifie :

« x et y sont racines d'un même polynôme irréductible sur K ».

Le nombre de conjugués d'un élément algébrique sur K est, on l'a dit, égal à son degré, et les éléments de K sont les seuls qui n'ont pas d'autre conjugué qu'eux-mêmes.

Si l'on « restreint le cadre » en se plaçant dans le corps de rupture L d'un polynôme sur K , alors les éléments de K sont caractérisés par le fait d'être les seuls fixes par tous les K -automorphismes de L : conséquence immédiate de ce qui précède.

Les éléments du corps de base sont les seuls fixes par le groupe de Galois d'un polynôme.

On verra plus loin pourquoi L doit être un *corps de rupture* et non une extension arbitraire (même de degré fini) de K .

Une remarque

En partant d'un K -automorphisme σ , on peut construire un exemple où z est un élément (comme M_2) multiple de z . Il y a mieux, alors la suite nombre des $\sigma^i(z)$ ne se répète pas. Il reste

où z est un élément (comme M_2) multiple de z . Il y a mieux, alors la suite nombre des $\sigma^i(z)$ ne se répète pas. Il reste

Soit par exemple e racine n -ième de l'unité dans $K[X]$ et le quotient de $X^n - 1$ par $X - 1$ est donc est correct. On é

Ce nombre est le quotient de $X^n - 1$ par $X - 1$. On prend le minimum, et le polynôme « Φ_n » répète, cha

montré que la
se vérifie

Une remarque sur les conjugués.

En particulier, si un polynôme $P \in L[X]$ est fixe par tous les K -automorphismes de L , ses coefficients sont dans K .

Un exemple simple est donné par le polynôme

$$T_z(X) = \prod_{\sigma \in G(L|K)} (X - \sigma(z))$$

où z est un élément donné de L , de polynôme minimum M_z . Le polynôme T_z est (comme M_z) à coefficients dans K , car fixe par tout le groupe de Galois, et il est multiple de M_z dans $K[X]$.

Il y a mieux : si $(z_1, \dots, z_p)$ est la suite des racines de M_z , donc des conjugués de z , alors la suite des $\sigma(z)$ est formée des éléments z_i chacun répétés. Appelons n_i le nombre de $\sigma(z)$ égaux à z_i .

Il reste

$$M_z = \prod_{i=1}^p (X - z_i)$$

$$T_z = \prod_{i=1}^p (X - z_i)^{n_i}.$$

Soit par exemple n_1 le plus petit des n_i . Alors T_z est multiple de $(M_z)^{n_1}$ dans $K[X]$ et le quotient n'a pas z_1 pour racine. Il ne peut donc avoir aucun des z_i pour racine (car les z_i sont conjugués sur K), ce qui entraîne qu'il n'a pas de racine, donc est constant. D'où l'égalité $T_z = (M_z)^{n_1}$ qui montre que les n_i sont tous égaux. On énoncera :

La suite des conjugués d'un élément par rapport à un corps de rupture (ou un polynôme) est formée des conjugués de cet élément répétés chacun un nombre égal de fois.

Ce nombre de fois est d'ailleurs le quotient des degrés de T_z et de M_z , donc le quotient de $L : K$ et de $K(z) : K$, il est égal au degré de L sur $K(z)$.

On prendra donc garde à ne pas faire de confusion en parlant des « conjugués d'un élément algébrique z », c'est-à-dire l'ensemble des racines de son polynôme minimum, et des « conjugués de z dans tel corps de rupture ou par rapport à tel polynôme » : c'est alors une suite où les conjugués dans le premier sens se répètent, chacun autant de fois.

- Ainsi, si $x = \sqrt[3]{2}$ est la racine cubique réelle de 2, son polynôme minimum est

$$M_x = X^3 - 2$$

sur $\mathbb{Q}$, donc ses conjugués sur $\mathbb{Q}$ sont x, jx et j^2x . Mais si l'on se place dans un corps de rupture, le « plus petit » est le corps de rupture $\mathbb{Q}(x, j)$ de $X^3 - 2$, qui est de degré 6 sur $\mathbb{Q}$: les conjugués de x par rapport à son polynôme minimum forment donc la suite

$$(x, x, jx, jx, j^2x, j^2x).$$

Chacun est répété deux fois car 2 est le degré du corps de rupture sur $\mathbb{Q}(x)$.

• On peut aussi prendre pour cadre le corps de rupture du polynôme

$$(X^3 - 2)(X^2 + 1) = X^5 + X^3 - 2X^2 - 2.$$

Le corps de rupture contient x , il est égal à $\mathbb{Q}(x, j, i)$, et de degré 12 car i est de degré 2 sur $\mathbb{Q}(x, j)$ (pourquoi ?). Les conjugués de x par rapport à ce polynôme forment alors la suite de longueur 12, les éléments x, jx, j^2x étant chacun répété quatre fois.

D'où le

Les autres T_i .

Une propriété caractéristique du groupe de Galois.

Partons d'un polynôme P sur le corps K et appelons $\alpha_1, \dots, \alpha_n$ ses racines, que l'on supposera simples s'il le faut.

L'effet des permutations sur l'ensemble de ces racines peut se traduire sur l'élément

$$\theta = \alpha_1 X_1 + \dots + \alpha_n X_n$$

où les X_i sont des indéterminées : effectuer une permutation σ sur les X_i revient à effectuer la permutation σ^{-1} sur les α_i .

Pour tout $\sigma \in \Sigma_n$, on posera donc

$$\sigma\theta = \alpha_1 X_{\sigma(1)} + \dots + \alpha_n X_{\sigma(n)}.$$

On introduit encore une indéterminée X et on forme le polynôme dont les racines (en X) sont les $\sigma\theta$: c'est

$$T = \prod_{\sigma \in \Sigma_n} (X - \sigma\theta) \in K[X_1, \dots, X_n, X]$$

car les coefficients sont dans K puisque ce sont des fonctions symétriques des racines de P .

On le décompose en facteurs premiers

$$T = T_1 \dots T_m$$

en supposant par exemple que c'est T_1 qui contient le facteur $X - \theta$.

Si une permutation $s \in \Sigma_n$ est dans le groupe de Galois de P sur K , elle définit un K -autoisomorphisme du corps de rupture $K(\alpha_1, \dots, \alpha_n)$, qui possède un unique prolongement en K -automorphisme de l'anneau des polynômes : dans ces conditions T_1 est fixe par s .

Inversement, supposons qu'une permutation $\tau \in \Sigma_n$ laisse T_1 fixe. Alors $X - \tau\theta$ est un facteur de T_1 , donc $\tau\theta$ est un conjugué de θ sur K , d'où un K -automorphisme de $K(\alpha_1, \dots, \alpha_n)$ correspondant à la permutation τ^{-1} des α_i : dès lors τ^{-1} , donc τ , est dans le groupe de Galois de P sur K .

Le critère d'application

Ainsi, par exemple, à 1. Ce polynôme sur le corps $\mathbb{Q}$ même degré cyclique, en fait égales aux deux imaginer (voir

Quelle relation sur $\mathbb{Q}$? Le critère

En effet, a est un produit, laisse fixe les coefficients, elle transforme

Deux remarques

• on a pu (pour cause

• il faut l'appliquer bien que P n'est pas une racine

On énonce

Appliquée à l'exemple précédent, on a les exemples suivants :

D'où le critère suivant :

Le groupe de Galois de P sur K est formé des permutations des racines $\alpha_1, \dots, \alpha_n$ qui laissent fixe l'un des facteurs premiers du polynôme

$$\prod_{\sigma \in \Sigma_n} (X - \sigma\theta)$$

où l'on a posé

$$\sigma\theta = \alpha_1 X_{\sigma(1)} + \dots + \alpha_n X_{\sigma(n)}.$$

Les autres permutations (les « mauvaises ») transforment T_1 en un autre des T_i .

Quand on passe au quotient.

Le critère précédent n'est pas bien utile en soi. Mais il est utile car son application dans certains cas donne des renseignements sur le groupe de Galois.

Ainsi, partons d'un polynôme P à coefficients entiers, le dominant étant égal à 1. Ce polynôme sur le corps $\mathbb{Q}$ donne, par passage au quotient, un polynôme $\bar{P}$ sur le corps $\mathbb{Z}/q$ des entiers modulo le nombre premier q . Bien entendu, P et $\bar{P}$ ont même degré, soit n . Mais le groupe de Galois de $\bar{P}$ sur $\mathbb{Z}/q$ est facile : il est cyclique, engendré par un produit de cycles disjoints de longueurs respectives égales aux degrés des facteurs premiers de $\bar{P}$ dans $\mathbb{Z}/q$ [c'est plus long à écrire qu'à imaginer (voir p. 166)].

Quelle relation y a-t-il entre le groupe de Galois de $\bar{P}$ sur $\mathbb{Z}/q$ et celui de P sur $\mathbb{Q}$? Le critère ci-dessus montre que le premier est un sous-groupe du second :

$$G(\bar{P}|\mathbb{Z}/q) \subset G(P|\mathbb{Q}).$$

En effet, avec les mêmes notations, on passe modulo q et on remarque que $\bar{T}_1$ est un produit de facteurs premiers de $\bar{T}$ modulo q , donc toute permutation qui laisse fixe les facteurs premiers de $\bar{T}$ modulo q laisse fixe *a fortiori* T_1 (car sinon elle transformerait T_1 en un autre T_i).

Deux remarques :

- on a pu passer au quotient modulo q car T est aussi à coefficients entiers (pour cause de fonctions symétriques des racines);
- il faut l'hypothèse supplémentaire que $\bar{P}$ n'ait pas de racines multiples (car bien que P n'en ait pas, $\bar{P}$ peut en avoir : ainsi 1 est racine simple de $X^2 - 1$ sur $\mathbb{Q}$, mais racine double de $X^2 - 1$ sur $\mathbb{Z}/2$).

On énoncera :

Si $P \in \mathbb{Z}[X]$ a 1 pour coefficient dominant, si dans un corps $\mathbb{Z}/q$ ses racines sont simples et ses facteurs premiers de degrés $n_1, \dots, n_r$, alors le groupe de Galois de P sur $\mathbb{Q}$ contient un produit de cycles disjoints de longueurs respectives $n_1, \dots, n_r$.

Appliquée pour diverses valeurs de q , cette méthode donne souvent des renseignements utiles sur le groupe de Galois cherché (en particulier quand les exemples sont truqués...).

Aucun intérêt, bien sûr, si P est totalement factorisable modulo q . Par contre, si P est irréductible modulo un certain q , le groupe de Galois de P contient un cycle de longueur égale à son degré.

• Ainsi partons de

$$X^3 + 3X + 1$$

pour étudier son groupe de Galois G sur $\mathbb{Q}$.

Modulo 2, on trouve

$$X^3 + X + 1$$

sans racines dans $\mathbb{Z}/2$, donc irréductible : G contient un cycle d'ordre 3, donc G contient A_3 , ce qui montre déjà que

$$X^3 + 3X + 1$$

est irréductible sur $\mathbb{Q}$.

Si l'on trouve un q tel que le polynôme ait une seule racine dans $\mathbb{Z}/q$, et simple de surcroît, alors G contiendra une transposition, donc sera égal à Σ_3 .

Modulo 3, l'égalité

$$X^3 + 1 = (X + 1)^3$$

ne donne rien.

Modulo 5, on trouve

$$X^3 - 2X + 1 = (X - 1)(X - 2)^2 :$$

aucun intérêt.

Modulo 7, on écrit

$$X^3 + 3X + 1 = (X - 4)(X^2 + 4X - 2)$$

et le second facteur a pour discriminant 4×6 ; or 6 n'est pas un carré dans $\mathbb{Z}/7$ (il suffit d'écrire la liste des carrés, qui comprend 1, 2, 4), donc on a bien ici un cycle de longueur 2, c'est-à-dire une transposition.

En conclusion,

$$G(X^3 + 3X + 1 | \mathbb{Q}) = \Sigma_3$$

résultat déjà démontré directement (voir p. 151).

Une précision sur l'équation binôme.

On a montré que, sur un corps K contenant les racines n -ièmes de l'unité, le groupe de Galois de $X^n - a$ est un sous-groupe du groupe cyclique C_n ; donc l'ordre de ce groupe, qui est aussi le degré d du corps de rupture, est un diviseur de n . Que peut-on dire de plus sur ce degré ?

Appelons
hypothèse
notera K
s'écrit

les m_i éta
l'unité, d
Le pro
au signe
Comm
donc $\alpha^d \in$
On a m
possède u
 n -ièmes d

Comm
que c'est l
 $\alpha^{nq} = b^n$,
donc que
sur K ; or

Et si K

où ω est
cyclotomi
rupture es
on montr

1. Par contre,
contient un

Appelons ω une racine primitive n -ième de l'unité, contenue dans K par hypothèse. Le corps de rupture est engendré par toute racine n -ième de a , on le notera $K(\sqrt[n]{a})$. En appelant α l'une de ces racines, les d conjugués de α sur K s'écrivent

$$\alpha_1 = \alpha, \quad \alpha_2 = \alpha\omega^{m_1}, \quad \alpha_3 = \alpha\omega^{m_2}, \dots, \alpha_d = \alpha\omega^{m_{d-1}}$$

les m_i étant des entiers (car le quotient de deux racines est une racine n -ième de l'unité, donc une puissance de ω).

Le produit de ces conjugués est une fonction symétrique, donc est dans K (c'est au signe près le terme constant du polynôme minimum de α sur K).

ent un cycle
que

Comme ω est déjà dans K , on en déduit $\alpha^d \in K$. Or α est racine n -ième de a , donc α^d est racine n -ième de a^d .

On a montré que si d est le degré du corps de rupture de $X^n - a$ sur K , alors a^d possède une racine n -ième dans K (attention : K contient toujours les racines n -ièmes de l'unité).

racine dans
transposition,

Comment caractériser d parmi les entiers q vérifiant $\sqrt[n]{a^q} \in K$? On va montrer que c'est le plus petit. En effet, soit un tel q ; il existe alors $b \in K$ avec $a^q = b^n$, d'où $\alpha^{nq} = b^n$, ce qui montre que α^q est produit de b par une racine n -ième de l'unité, donc que α^q est dans K et enfin que α est racine d'une équation binôme de degré q sur K ; or α est de degré d sur K , d'où l'inégalité $q \geq d$.

Le degré du corps de rupture de $X^n - a$ sur un corps K contenant les racines n -ièmes de l'unité est la plus petite puissance de a qui possède une racine n -ième dans K .

Et si K ne contient pas les racines n -ièmes de l'unité ? On écrit alors la chaîne

$$K \subset K(\omega) \subset L = K(\omega, \sqrt[n]{a})$$

6 n'est pas
qui comprend
est-à-dire une

où ω est une racine n -ième primitive de l'unité et $K(\omega)$ est appelé corps cyclotomique d'indice n . Par multiplicativité, on trouve que le degré du corps de rupture est le degré ci-dessus multiplié par le degré du corps cyclotomique (sur $\mathbb{Q}$, on montre que c'est le nombre d'entiers inférieurs à n premiers avec n).

Ainsi, prenons $X^{12} - 4$ sur $\mathbb{Q}$. Ses racines sont les produits de $\sqrt[6]{2}$ par les racines douzièmes de l'unité, donc par les puissances de ij .

Le corps de rupture est donc

$$\mathbb{Q}(\sqrt[6]{2}, ij)$$

de degré 24 sur $\mathbb{Q}$ et de degré 6 sur $\mathbb{Q}(ij) = \mathbb{Q}(i, j)$.

Conclusions :

- $G(X^{12} - 4 | \mathbb{Q}(i, j)) = C_6$
- la plus petite puissance de 4 qui possède une racine douzième dans $\mathbb{Q}(i, j)$ est la sixième.

de l'unité, le
cyclique C_n ;
pture, est un

L'équation dite bicarrée.

Une équation « bicarrée » correspond, par définition, à un polynôme pair de degré 4, soit

$$P = X^4 + aX^2 + b \in K[X].$$

Ses racines s'écrivent

$$\pm \sqrt{\frac{-a \pm \sqrt{a^2 - 4b}}{2}}$$

on les notera dorénavant $(\alpha_1, \alpha_2, -\alpha_1, -\alpha_2)$. Elles vérifient donc

$$\alpha_1^2 + \alpha_2^2 = -a \quad \text{et} \quad \alpha_1^2 \alpha_2^2 = b$$

et le corps de rupture est engendré par une des racines de P et une racine carrée de b .

On ne va examiner que le cas où P est irréductible. Or un polynôme pair de degré 4 est irréductible s'il a un facteur de degré 1 ou deux facteurs irréductibles de degré 2. Dans le premier cas il est clair qu'il a un facteur de la forme $X^2 - t^2$, avec $t \in K$, alors que dans le second cas l'unicité de la décomposition en facteurs premiers montre, par la substitution de X en $-X$, que la décomposition doit être de l'une des formes :

$$X^4 + aX^2 + b = (X^2 + uX + v)(X^2 - uX + v)$$

ou

$$X^4 + aX^2 + b = (X^2 + s)(X^2 + t).$$

La seconde signifie que

$$X^2 + aX + b$$

possède une racine dans K , ce qui s'écrit $\sqrt{a^2 - 4b} \in K$. La première donne

$$\begin{cases} v^2 = b \\ 2v - u^2 = a \end{cases}$$

ce qui s'écrit $\sqrt{2\sqrt{b} - a} \in K$, où $\sqrt{b}$ est l'une des racines carrées de b (l'autre ne marche pas forcément, comme le montre l'exemple de $X^4 + 4$ sur $\mathbb{Q}$).

On va donc supposer désormais

$$\sqrt{a^2 - 4b} \notin K \quad \text{et} \quad \sqrt{2\sqrt{b} - a} \notin K.$$

Dans ces conditions, toute racine est de degré 4 sur K , puisque P est le polynôme minimum, donc le degré du corps de rupture sera 4 ou 8 suivant que $\sqrt{b}$ sera dans $K(\alpha_1)$ ou hors de $K(\alpha_1)$.

Dans la première hypothèse toute racine engendre le corps de rupture, le groupe de Galois est C_4 ou $C_2 \times C_2$: un exemple est donné par $X^4 + 9$ sur $\mathbb{Q}$, dont le corps de rupture est $\mathbb{Q}(i, \sqrt{6})$, de degré 4, et le groupe de Galois est $C_2 \times C_2$ (les racines étant $\frac{\pm 1 \pm i}{2} \sqrt{6}$).

LES CON

Le seco
n'étant pr

On tro
algébrique
Galois de
de ruptur.

Comme
corps de r
de α_1 , qui

Pour α_1

Si α_1 est
doit en être
tout (donc
(1 3) (2 4)

Quant à
 α_1 en α_2 et
(1 3) (2 4)
 $\sigma(-\alpha_1) =$

Examin

• $\sigma(\alpha_2)$
de

C'est le
commuten
groupe, ce

• $\sigma(\alpha_2)$

C'est le gro
d'ordre 4. I
dès qu'il le
- α_1 , donc
se calcule :

(
d'où l'on d

On a m
le corps de

La récip
être ensembl
ou bien α_1

est dans K

polynôme pair de

Le second cas, lui, correspond à un corps de rupture de degré 8, aucune racine n'étant primitive, ce qui s'écrit encore $\alpha_2 \notin K(\alpha_1)$.

On trouve l'exemple de l'« équation bicarrée générale », celle où a et b sont algébriquement indépendants. Plus concrètement, on a vu que le groupe de Galois de $X^4 - 2$ sur $\mathbb{Q}$ est d'ordre 8 (groupe D_8 des isométries du carré), le corps de rupture étant $\mathbb{Q}(i, \sqrt[4]{2})$.

Commençons par étudier le premier cas. Comme α_1 est élément primitif du corps de rupture, il y a quatre bonnes permutations, données chacune par l'image de α_1 , qui est $\alpha_1, -\alpha_1, \alpha_2$, ou $-\alpha_2$.

onc

Pour α_1 fixe, on trouve bien sûr id.

ne racine carrée

Si α_1 est transformé en $-\alpha_1$, les deux racines α_1 et $-\alpha_1$ sont échangées et il doit en être de même de α_2 et $-\alpha_2$ car α_2 est aussi élément primitif et, s'il était fixe, tout (donc α_1) le serait. Bref, le groupe de Galois $G(P)$ contient déjà id et $(1\ 3)(2\ 4)$.

polynôme pair de
rs irréductibles
forme $X^2 - t^2$.
tion en facteurs
composition doit

Quant aux deux autres bonnes permutations, il y a celle, σ , qui transforme α_1 en α_2 et celle qui transforme α_1 en $-\alpha_2$ et n'est autre que le produit de σ par $(1\ 3)(2\ 4)$. Tout revient à calculer $\sigma \in G(P)$ telle que $\sigma(\alpha_1) = \alpha_2$; on a bien sûr $\sigma(-\alpha_1) = -\alpha_2$, donc pour $\sigma(\alpha_2)$ il reste, soit α_1 , soit $-\alpha_1$.

Examinons les deux éventualités.

v)

• $\sigma(\alpha_2) = \alpha_1$: alors σ s'écrit $(1\ 2)(3\ 4)$ et le groupe de Galois $G(P)$ est formé de

$$\text{id}, (1\ 3)(2\ 4), (1\ 2)(3\ 4), (1\ 4)(2\ 3).$$

C'est le groupe $C_2 \times C_2$ engendré par deux éléments d'ordre 2 qui commutent. Comment reconnaître ce cas ? On vérifie que $\alpha_1\alpha_2$ est fixe par le groupe, ce qui exige $\sqrt{b} \in K$ car tout élément fixe est dans le corps de base.

remière donne

• $\sigma(\alpha_2) = -\alpha_1$: ici, σ s'écrit $(1\ 2\ 3\ 4)$, et $G(P)$ est formé de

$$\text{id}, (1\ 3)(2\ 4), (1\ 2\ 3\ 4), (1\ 4\ 3\ 2).$$

s de b (l'autre ne
sur $\mathbb{Q}$).

C'est le groupe cyclique C_4 , engendré par l'une des deux permutations cycliques d'ordre 4. Pour reconnaître ce cas, on remarque qu'un élément sera fixe par $G(P)$ dès qu'il le sera par le générateur $\sigma = (1\ 2\ 3\ 4)$, qui transforme α_1 en α_2 et α_2 en $-\alpha_1$, donc laisse fixe $\alpha_1\alpha_2(\alpha_1^2 - \alpha_2^2)$. Cet élément doit être dans K . Or son carré se calcule facilement :

$$(\alpha_1\alpha_2)^2(\alpha_1^2 - \alpha_2^2)^2 = b[(\alpha_1^2 + \alpha_2^2)^2 - 4\alpha_1^2\alpha_2^2] = b(a^2 - 4b)$$

d'où l'on déduit $\sqrt{b(a^2 - 4b)} \in K$.

uisque P est le
u 8 suivant que

On a montré :

le corps de rupture est de degré 4 $\Rightarrow \sqrt{b} \in K$ ou $\sqrt{b(a^2 - 4b)} \in K$.

s de rupture, le
r $X^4 + 9$ sur $\mathbb{Q}$,
e de Galois est

La réciproque est facile : si $\sqrt{b}$ ou $\sqrt{b(a^2 - 4b)}$ est dans K (et ils ne peuvent y être ensemble, car leur quotient n'est pas dans K à cause de l'irréductibilité), alors ou bien $\alpha_1\alpha_2$ est dans K , et alors α_2 est dans $K(\alpha_1)$, ou bien

$$\alpha_1\alpha_2(\alpha_1^2 - \alpha_2^2) = \alpha_1\alpha_2(a + 2\alpha_1^2)$$

est dans K , et l'on a encore $\alpha_2 \in K(\alpha_1)$.

Autrement dit, le corps de rupture sera de degré 8 si, et seulement si, le corps de base ne contient ni $\sqrt{b}$ ni $\sqrt{b(a^2 - 4b)}$; en ce cas, $\alpha_1 + \alpha_2$ n'est pas élément primitif non plus, mais on a vu que $\alpha_1 + 2\alpha_2$ l'est toujours (voir p. 108).

On peut donc écrire

$$\begin{aligned}\sqrt{b} \in K &\Leftrightarrow G(P) = C_2 \times C_2 \\ \sqrt{b(a^2 - 4b)} \in K &\Leftrightarrow G(P) = C_4 \\ \sqrt{b} \notin K \text{ et } \sqrt{b(a^2 - 4b)} \notin K &\Leftrightarrow G(P) \text{ est d'ordre } 8.\end{aligned}$$

Dans ce dernier cas (qui est celui qui se produit quand a et b sont des indéterminées sur un corps), le groupe de Galois contient :

- l'identité;
- l'échange d'un ou de deux couples de racines opposées entre elles, soit (1 3), (2 4) et (1 3)(2 4);
- l'échange de chacune des racines $\{\alpha_1, -\alpha_1\}$ avec chacune des deux autres, soit

$$(1\ 2)(3\ 4) \quad \text{et} \quad (1\ 4)(2\ 3);$$

- les deux cycles d'ordre 4, (1 2 3 4) et (1 4 3 2).

C'est là le groupe D_8 des isométries du carré, les deux dernières étant les rotations d'ordre 4, (1 3)(2 4) la rotation de π , et les quatre autres éléments d'ordre 2 étant les symétries par rapport à des médiatrices ou diagonales.

Un retour en arrière : Lagrange.

Bien avant Galois, Lagrange avait déjà obtenu des résultats importants, surtout en ce qui concerne l'équation générale. Il avait en particulier déjà compris l'importance du rôle des permutations des racines.

Ses deux résultats essentiels, faciles à traduire maintenant en termes de conjugués, étaient les suivants : on part du polynôme P de degré n (pour Lagrange, c'était l'équation générale) et de racines $x_1, \dots, x_n$. Lagrange disait que la fonction rationnelle des racines $T(x_1, \dots, x_n)$, à coefficients dans K , admet la permutation $\sigma \in \Sigma_n$ quand elle vérifie

$$T(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = T(x_1, \dots, x_n).$$

Il a alors démontré, à l'aide de méthodes plus artisanales, que :

- si toute permutation admise par $T(x_1, \dots, x_n)$ est admise aussi par $S(x_1, \dots, x_n)$, alors $S(x_1, \dots, x_n)$ s'exprime rationnellement à l'aide de K et de $T(x_1, \dots, x_n)$;
- si $S(x_{\sigma(1)}, \dots, x_{\sigma(n)})$ prend m valeurs distinctes quand σ parcourt toutes les permutations admises par $T(x_1, \dots, x_n)$, alors $S(x_1, \dots, x_n)$ est racine d'un polynôme de degré m dont les coefficients s'expriment rationnellement à l'aide de K et de $T(x_1, \dots, x_n)$.

Bien entendu, le premier résultat est un cas particulier du second ($m = 1$). A l'aide de la notion de conjugués, ces résultats sont faciles à démontrer.

Appelo

qui appar
L'ensen
groupe de
Dire qu
par le grou
résultat.

Quant
donc que
de degré

Dans ce
construisa

où T_1 est s
A chaq
dans le cor
prises par
 $T_{i-1}(x_1, \dots$

Les éq
résolvante
d'une équ
binômes.

le corps de
pas élément
n. 108).

Appelons en effet α et β respectivement les éléments

$$S(x_1, \dots, x_n) \quad \text{et} \quad T(x_1, \dots, x_n)$$

qui appartiennent au corps de rupture de P sur K .

L'ensemble des « permutations admises par $T(x_1, \dots, x_n)$ » n'est autre que le groupe de Galois de P sur $K(\beta)$.

Dire que ces permutations sont admises par $S(x_1, \dots, x_n)$ signifie que α est fixe par le groupe de Galois de P sur $K(\beta)$, ce qui s'écrit $\alpha \in K(\beta)$ et montre le premier résultat.

b sont des

Quant au second, l'hypothèse signifie que α possède m conjugués sur $K(\beta)$, donc que α est de degré m sur $K(\beta)$, c'est-à-dire racine d'un polynôme irréductible de degré m à coefficients dans $K(\beta)$.

elles, soit

Dans ces conditions, Lagrange cherchait à résoudre l'équation $P(X) = 0$ en construisant une suite de fonctions rationnelles des racines de la forme

eux autres.

$$T_1(x_1, \dots, x_n), \quad T_2(x_1, \dots, x_n), \quad \dots, \quad T_q(x_1, \dots, x_n)$$

où T_1 est symétrique (donc dans le corps de base) et $T_q(x_1, \dots, x_n)$ est égale à x_1 .

es étant les
s éléments
onales.

A chaque étape, $T_i(x_1, \dots, x_n)$ vérifiait une équation de degré m_i à coefficients dans le corps engendré par les précédents, m_i étant le nombre de valeurs distinctes prises par $T_i(x_1, \dots, x_n)$ quand on applique toutes les substitutions admises par $T_{i-1}(x_1, \dots, x_n)$.

Ainsi, la résolution de l'équation générale de degré 4 correspond à la suite

$$1, \quad x_1x_2 + x_3x_4, \quad x_1x_2, \quad x_1$$

mportants,
culier déjà

L'élément $\alpha = x_1x_2 + x_3x_4$ admet les huit substitutions

$$\text{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4), \\ (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3)$$

termes de
ré n (pour
ange disait
is K , admet

et il prend trois valeurs distinctes sur les vingt-quatre substitutions possibles. On en déduit d'abord que α est racine d'une équation de degré 3 sur K .

Mais par les huit substitutions ci-dessus on ne trouve que deux valeurs distinctes pour x_1x_2 , ce sont x_1x_2 et x_3x_4 , donc x_1x_2 est racine d'une équation de degré 2 à coefficients dans $K(\alpha)$.

aussi par
de K et de

Enfin x_1x_2 n'admet que id et $(1\ 2)$, d'où deux valeurs pour x_1 .

t toutes les
racine d'un
à l'aide de

C'est ainsi que se trouve ramenée la résolution de l'équation de degré 4 à des équations de degrés 3 et 2.

d ($m = 1$).
entrer.

Les équations dont les $T_i(x_1, \dots, x_n)$ étaient racines s'appelaient les **résolvantes partielles**. Et tout le problème de l'expression algébrique des racines d'une équation se réduit à la recherche d'une suite de résolvantes partielles **binômes**.

Exercices.

1. Dans le corps de rupture de

$$X^3 - 3X + 1$$

sur $\mathbb{Q}$, on prend comme élément primitif la différence de deux racines.

Montrer que l'on trouve comme polynôme minimum, soit

$$X^3 - 9X + 9,$$

soit

$$X^3 - 9X - 9.$$

En déduire que le groupe de Galois de $X^3 - 3X + 1$ sur $\mathbb{Q}$ est cyclique, d'ordre 3.

2. Trouver, pour le corps de rupture de

$$X^4 - 5X^2 + 6$$

sur $\mathbb{Q}$, un élément primitif combinaison $\mathbb{Q}$ -linéaire des racines.

Écrire une telle combinaison $\mathbb{Q}$ -linéaire qui prend $4! = 24$ valeurs distinctes sur les permutations des quatre racines. Montrer que ce n'est pas le cas de $\sqrt{2} + \sqrt{3}$, mais que c'est tout de même un élément primitif car les valeurs sont distinctes si l'on se limite au groupe de Galois.

3. Soit
- $K(x)$
- un corps de rupture sur
- K
- . Si
- y
- est dans
- $K(x)$
- et si
- $K(y)$
- contient tous les conjugués de
- y
- , alors le groupe de Galois de
- $K(y)$
- sur
- K
- est image par un homomorphisme du groupe de Galois de
- $K(x)$
- sur
- K
- .

4. Étudier les groupes de Galois, sur
- $\mathbb{Q}$
- , de

$$X^4 - 5X^2 + 6, \quad X^4 + X^2 + 1, \quad X^4 + 1, \quad X^3 + X^2 - 2X - 1, \\ X^4 + 3X^3 - 3X - 2 \quad \text{et} \quad X^5 - X - 1.$$

5. Établir d'abord les deux résultats préliminaires suivants :

• si un sous-groupe transitif de Σ_n contient une transposition et un cycle de longueur $(n - 1)$, il est égal à Σ_n tout entier (on montrera par des conjugaisons que le sous-groupe contient toutes les transpositions);

• pour tout n et tout nombre premier q , il existe un polynôme de degré n irréductible dans $\mathbb{Z}/q$ (on considérera le polynôme minimum sur $\mathbb{Z}/q$ d'un élément primitif du corps de Galois de cardinal q^n).

Dans ces conditions, étant donné $n > 3$, on justifiera l'existence des polynômes suivants, à coefficients entiers, le dominant égal à 1 :

- un polynôme P_1 de degré n irréductible modulo 2;
- un polynôme P_2 de degré n ayant, modulo 3, un facteur irréductible de degré $(n - 1)$;
- un polynôme P_3 de degré n dont les facteurs premiers modulo 5 sont un facteur de degré 2 et un ou deux facteurs de degré impair.

On posera ensuite $P = -15P_1 + 10P_2 + 6P_3$.

On montrera que P est irréductible sur $\mathbb{Z}/2$, sur $\mathbb{Q}$, et que son groupe de Galois contient un cycle d'ordre $(n - 1)$ et un produit σ d'une transposition et de cycles disjoints d'ordres impairs. Il existe alors un entier m impair tel que σ^m soit une transposition. On en déduira que le groupe de Galois de P sur $\mathbb{Q}$ est Σ_n tout entier.

En conclusion, pour tout entier n , il existe un polynôme irréductible sur $\mathbb{Q}$ dont le groupe de Galois est Σ_n tout entier.

6. On appelle élément primitif l'élément
- α
- d'un corps
- K
- d'ordre
- n
- tel que
- $K = K(\alpha)$
- . Donner c

X

Pour l'éq

montrer, trouve po

$R = X^6 -$

Vérifier q décompos P :

7. Un polynôme engendre l'engendré

Montrer c

• toutes l

• toutes l

• l'ordre c

• le degré

Vérifier les

• tout pol

• un poly base conti

• le polyn de base cc

• si le gro normal (or égale au d

• si le gro normal (or transitif G tout i entr

Étudier le

6. On appelle **résolvante de Galois** d'un polynôme tout polynôme minimum d'un élément primitif du corps de rupture. Montrer que le degré de la résolvante est l'ordre du groupe de Galois, et que la résolvante a même groupe de Galois que le polynôme.

Donner des exemples de résolvantes de Galois pour

$$X^3 - 2, \quad X^4 + 2, \quad X^3 + X^2 + X + 1, \quad X^3 + pX + q.$$

Pour l'équation générale de degré 3,

$$P = X^3 + a_1X^2 + a_2X + a_3$$

montrer, en prenant pour élément primitif la différence de deux racines, que l'on trouve pour résolvante de Galois

$$R = X^6 + 2(3a_2 - a_1^2)X^4 + (3a_2 - a_1^2)^2X^2 - a_1^2a_2^2 - 18a_1a_2a_3 + 4a_1^3a_3 + 4a_2^3 + 27a_3^2.$$

Vérifier que le discriminant de P est l'opposé du terme constant de R , et que R se décompose si l'on adjoint au corps de base une racine carrée δ du discriminant de P :

$$R = [X^3 + (3a_2 - a_1^2)X + \delta][X^3 + (3a_2 - a_1^2)X - \delta].$$

7. Un polynôme est dit **normal** quand il est irréductible et quand l'une de ses racines engendre le corps de rupture (si l'on ne précise pas le corps de base, ce sera le corps engendré par les coefficients).

Montrer qu'il est équivalent de donner l'une des conditions suivantes :

- toutes les racines sont éléments primitifs du corps de rupture ;
- toutes les racines s'expriment rationnellement à l'aide de l'une d'elles ;
- l'ordre du groupe de Galois est le degré du polynôme ;
- le degré de toute résolvante de Galois (voir ci-dessus) est le degré du polynôme.

Vérifier les affirmations suivantes :

- tout polynôme irréductible de degré 2 est normal ;
- un polynôme irréductible de degré 3 est normal si, et seulement si, le corps de base contient une racine carrée du discriminant ;
- le polynôme $X^p - a$ supposé irréductible est normal si, et seulement si, le corps de base contient les racines p -ièmes de l'unité (p premier) ;
- si le groupe de Galois d'un polynôme irréductible est cyclique, le polynôme est normal (on justifiera la génération du groupe de Galois par un cycle de longueur égale au degré du polynôme) ;
- si le groupe de Galois d'un polynôme irréductible est abélien, le polynôme est normal (on ramènera le problème à la démonstration qu'un sous-groupe abélien transitif G de Σ_n est forcément d'ordre n , et pour le prouver on montrera que, pour tout i entre 1 et n , il existe un unique $\sigma \in G$ vérifiant $\sigma(1) = i$).

Étudier le caractère normal (sur $\mathbb{Q}$) des polynômes

$$X^3 + X^2 + X + 1; \quad X^4 - 5X^2 + 6; \\ X^4 - a \quad \text{et} \quad X^4 + aX^2 + b.$$

Extensions normales ou non

La caractérisation de la conjugaison en termes de racines du polynôme minimum inciterait à « faire éclater » le cadre des corps de rupture et à généraliser les notions précédentes à une extension arbitraire. On peut le faire, mais on « perd » alors certaines propriétés.

Les définitions.

Pour des éléments algébriques sur K , on définit la conjugaison à l'aide du polynôme minimum ; c'est une relation dans la clôture algébrique de K .

Des éléments conjugués sont des éléments ayant même polynôme minimum.

De même, le groupe de Galois peut se généraliser à une extension arbitraire.

Le groupe de Galois d'une extension est le groupe des automorphismes laissant fixe le corps de base.

On écrira encore $G(L|K)$ ou $G(L)$ le groupe de Galois de l'extension L de K ; ici, on ne le rattache plus aux permutations des racines d'un polynôme.

• Le groupe de Galois du corps $K(X)$ des fractions rationnelles est le groupe des K -automorphismes de $K(X)$. Un tel K -automorphisme est donné par l'image de X , qui doit être inversible pour la composition de fractions rationnelles, donc de la forme

$$\frac{aX + b}{cX + d} \quad \text{avec} \quad ad - bc \neq 0.$$

Tout $\varphi \in G(K(X)|K)$ est de la forme

$$\varphi : R(X) \rightarrow R\left(\frac{aX + b}{cX + d}\right)$$

et le groupe $G(K(X))$ est isomorphe au quotient du groupe $GL(2, K)$ des matrices inversibles 2×2 sur K (ou du groupe des permutations K -linéaires de K^2) par le sous-groupe K^* des homothéties non nulles.

En effet, a, b, c, d sont définis à un facteur non nul près.

Degré d'une exte

Pour un corp
l'extension. L'ex
générale et il nou
simples.

En effet, si l'or
nombre de conju
rupture du pol
transforment $\alpha \in$
n'est pas un cor

- Un exemple « éternel » est celui du corps $\mathbb{Q}(\sqrt[3]{2})$ obtenu en adjoignant à $\mathbb{Q}$ la racine cubique *réelle* de 2.

Ce corps est réel, et l'image de $\sqrt[3]{2}$ par tout automorphisme est une racine réelle de $X^3 - 2$: ce ne peut être qu'elle-même, le seul automorphisme est donc l'identité. On écrira

$$G(\mathbb{Q}(\sqrt[3]{2})) = \text{id}.$$

On notera qu'en ce cas les éléments du corps de base ne sont pas les seuls fixes par le groupe de Galois : tous le sont !...

- Autre exemple classique : le corps $\mathbb{Q}(\sqrt[4]{2})$, obtenu en adjoignant à $\mathbb{Q}$ la racine quatrième réelle positive de 2.

L'image de $\sqrt[4]{2}$ par un automorphisme est une racine réelle de $X^4 - 2$, c'est $\sqrt[4]{2}$ ou $-\sqrt[4]{2}$.

D'où le groupe de Galois

$$G(\mathbb{Q}(\sqrt[4]{2})) = C_2.$$

Le seul automorphisme autre que l'identité est

$$\lambda_0 + \lambda_1 u + \lambda_2 u^2 + \lambda_3 u^3 \rightarrow \lambda_0 - \lambda_1 u + \lambda_2 u^2 - \lambda_3 u^3$$

les λ_i étant rationnels, et u désignant $\sqrt[4]{2}$.

L'élément $\sqrt{2}$ est fixe par le groupe de Galois sans être dans le corps de base ; d'ailleurs, les éléments fixes par le groupe forment le corps intermédiaire $\mathbb{Q}(\sqrt{2})$.

Degré d'une extension et homomorphismes.

Pour un corps de rupture, l'ordre du groupe de Galois est égal au degré de l'extension. L'exemple de $\mathbb{Q}(\sqrt[3]{2})$ montre que ce n'est pas vrai pour une extension générale et il nous montre même le pourquoi, au moins dans le cas des extensions simples.

En effet, si l'on part d'une extension algébrique simple $K(\alpha)$, le degré n est le nombre de conjugués de α dans la clôture algébrique $\bar{K}$ de K (ou dans le corps de rupture du polynôme minimum de α). Les K -automorphismes de $K(\alpha)$ transforment α en un de ces conjugués, lequel doit être dans $K(\alpha)$. Or, si $K(\alpha)$ n'est pas un corps de rupture, α peut avoir des conjugués *hors* de $K(\alpha)$.

Exemple de $j\sqrt[3]{2}$ dans le cas de $\mathbb{Q}(\sqrt[3]{2})$.

les ou non

ines du polynôme
s de rupture et à
re. On peut le faire,

ugaison à l'aide du
ébrique de K .

ant même polynôme

extension arbitraire.

est le groupe des

l'extension L de K ;
un polynôme.

actions rationnelles
de $K(X)$. Un tel
de X qui doit être
rationnelles, donc de

$\neq 0$.

quotient du groupe
 K (ou du groupe des
ous-groupe K^* des

non nul près.

Pour voir de plus près, tout conjugué β de α définit un K -isomorphisme, par substitution

$$\begin{aligned} P(\alpha) &\rightarrow P(\beta) \\ K(\alpha) &\rightarrow K(\beta). \end{aligned}$$

Mais $K(\beta)$ est un sous-corps de $\bar{K}$ qui n'a aucune raison, bien que K -isomorphe, d'être égal à $K(\alpha)$.

Tout ce que l'on peut énoncer, dans le cas de degré fini (qui se ramène au cas ci-dessus en prenant un élément primitif) est :

Le degré d'une extension de degré fini est le nombre de K -homomorphismes de l'extension dans la clôture algébrique.

Le groupe de Galois d'une extension de degré fini.

Quant au groupe de Galois sur K de l'extension algébrique simple $K(\alpha)$, son ordre sera égal au nombre de conjugués de α (c'est-à-dire de racines de son polynôme minimum), contenus dans $K(\alpha)$.

En étendant à l'aide du théorème de l'élément primitif :

Pour une extension de degré fini, l'ordre du groupe de Galois est le nombre de conjugués d'un élément primitif contenus dans l'extension.

Une conséquence :

L'ordre du groupe de Galois est inférieur au degré de l'extension, et il ne lui est égal que si l'extension est un corps de rupture.

En effet, si α est un élément primitif, l'ordre du groupe de Galois est égal au degré $K(\alpha) : K$ si, et seulement si, tous les conjugués de α sont dans $K(\alpha)$; lequel $K(\alpha)$ est alors corps de rupture du polynôme minimum.

Une démonstration directe.

On peut, à titre de curiosité, donner une démonstration de la majoration de l'ordre du groupe par le degré de l'extension sans passer par un élément primitif.

Il suffit de montrer que, si L est de degré n sur K , il ne peut y avoir $(n + 1)$ K -automorphismes de L .

Tout d'abord, s'il y a $(n + 1)$ tels automorphismes, $\sigma_1, \dots, \sigma_{n+1}$, montrons qu'ils sont linéairement dépendants sur L .

Si $(u_1, \dots, u_n)$ est une base de L sur K , les $(n + 1)$ vecteurs suivants de L^n

$$\begin{aligned} v_1 &= (\sigma_1(u_1), \dots, \sigma_1(u_n)) \\ v_2 &= (\sigma_2(u_1), \dots, \sigma_2(u_n)) \\ &\dots\dots\dots \\ v_{n+1} &= (\sigma_{n+1}(u_1), \dots, \sigma_{n+1}(u_n)) \end{aligned}$$

sont linéairement indépendants.

On prend

par exemple les σ_i n'est pas

On applique les σ_i à α et on obtient des éléments différents. C

En combinant les résultats précédents, on voit que l'ordre du groupe de Galois ne peut être supérieur au degré de l'extension. Si l'ordre est égal au degré, l'extension est simple et son groupe de Galois est isomorphe à un groupe d'ordre n .

Le résultat précédent est un cas particulier du théorème de la clôture algébrique.

La notion de

Comme on voit, les extensions de degré fini sont linéairement indépendantes quand l'extension est simple.

On se propose de montrer que si L est un corps de rupture d'un polynôme $P(x)$, l'ordre du groupe de Galois est égal au degré de $P(x)$.

Inversément, si l'ordre du groupe de Galois est égal au degré de l'extension, celle-ci est simple et son groupe de Galois est isomorphe à un groupe d'ordre n .

Si L est une extension de degré n sur K , il est équivalent à :

• si un polynôme de degré n sur K se factorise dans L en facteurs irréductibles de degré 1.

• tout automorphisme de L sur K est déterminé par son action sur un élément primitif.

Une autre

rphisme, par

sont linéairement dépendants sur L et une relation de dépendance linéaire entre les v_i entraîne la même relation entre les σ_i .

On prend ensuite une relation de dépendance *minimale* entre les σ_i , soit

$$\lambda_1 \sigma_1 + \dots + \lambda_p \sigma_p = 0$$

n, bien que

par exemple ; les $\lambda_i \in L$ sont non nuls et aucune famille de moins de $(p - 1)$ parmi les σ_i n'est dépendante sur L .

ène au cas ci-

On applique à $x \in L$ et à $tx \in L$, où t est choisi tel que $\sigma_1(t)$ et $\sigma_p(t)$ soient différents. On écrit alors

nombre de
algébrique.

$$\begin{aligned} \lambda_1 \sigma_1(x) + \dots + \lambda_p \sigma_p(x) &= 0 \\ \lambda_1 \sigma_1(t) \sigma_1(x) + \dots + \lambda_p \sigma_p(t) \sigma_p(x) &= 0. \end{aligned}$$

En combinant, on trouve une dépendance linéaire entre $\sigma_2, \dots, \sigma_p$, ce qui contredit le caractère minimal de p . D'où l'impossibilité d'existence de $\sigma_1, \dots, \sigma_{n+1}$.

ple $K(\alpha)$, son
cines de son

Le résultat est bien démontré. D'ailleurs, cette dernière partie est un cas particulier de l'énoncé général : les endomorphismes non nuls d'un corps sont linéairement indépendants.

e Galois est le
ontenus dans

La notion d'extension normale.

Comme on vient de le voir, certaines anomalies peuvent se produire dans des extensions algébriques arbitraires, même de degré fini, alors que tout va bien quand l'extension est un corps de rupture.

l'extension, et
rupture.

On se place comme toujours en caractéristique nulle : alors le « secret » des corps de rupture est d'être saturés par conjugaison. En effet, si α est dans le corps de rupture de P sur K et si β a même polynôme minimum, on a montré que β est l'image de α par une permutation des racines de P , donc β est encore dans le corps de rupture (voir p. 164).

is est égal au
s $K(\alpha)$: lequel

Inversement, si une extension algébrique est saturée par conjugaison, on dit que c'est une extension **normale** ; elle est égale au corps de rupture du produit des polynômes minima d'une base quand son degré est fini.

Les corps de rupture sont les extensions normales de degré fini.

Si L est une extension algébrique de K , on écrit $K \triangleleft L$ quand elle est normale. Il est équivalent de donner l'une des caractérisations suivantes :

najoration de
ment primitif.
avoir $(n - 1)$

1, montrons

ivants de L

- si un polynôme irréductible sur K a une racine dans L , il y est totalement factorisable ;
- tout K -homomorphisme de L dans une extension est un K -automorphisme.

Une autre importante propriété :

En degré fini, les extensions normales sont celles dont le groupe de Galois est d'ordre égal au degré de l'extension.

Pour une extension non normale, le groupe de Galois a un ordre strictement inférieur au degré de l'extension. D'autres anomalies peuvent se produire ; ainsi les points fixes par le groupe de Galois forment un corps qui peut contenir *strictement* le corps de base.

- Toute extension quadratique est normale.
- Un corps algébriquement clos est extension normale (parfois de degré infini) de tous ses sous-corps.
- $\mathbb{R}$ n'est pas extension normale de $\mathbb{Q}$: le polynôme irréductible $X^3 - 2$ possède une racine seulement dans $\mathbb{R}$.

La clôture normale.

Pour une extension de degré fini, il existe manifestement une extension normale minimum la contenant : c'est le corps de rupture du produit des polynômes minima des éléments d'une base.

On l'appelle la **clôture normale** de l'extension.

- Le cas typique d'extension non normale est $\mathbb{Q}(\sqrt[3]{2})$, dont la clôture normale est

$$\mathbb{Q}(\sqrt[3]{2}, j) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}).$$

- La clôture normale de $\mathbb{Q}(\sqrt[4]{2})$ est $\mathbb{Q}(\sqrt[4]{2}, i)$.
- Si x est algébrique sur K , la clôture normale de $K(x)$ est $K(x_1, \dots, x_n)$, où les x_i sont tous les conjugués de x sur K .

Une utilisation de la clôture normale.

Soit α dans une extension L de degré fini de K . Pour tout K -homomorphisme de L dans la clôture algébrique $\bar{K}$ de K , l'image de α est bien sûr un conjugué de α (racine de son polynôme minimum).

En passant par la clôture normale, on peut montrer la réciproque. En effet, si β est un conjugué de $\alpha \in L$ sur K , alors le K -isomorphisme « substitution de α par β » de $K(\alpha)$ sur $K(\beta)$ se prolonge en un K -automorphisme de la clôture normale L_1 de L , puisque L_1 est un corps de rupture sur K contenant α et β . Si l'on restreint à L , on trouve un K -homomorphisme de L dans L_1 , donc dans $\bar{K}$.

Les conjugués sur K d'un élément d'une extension L de degré fini sont ses images par les K -homomorphismes de L dans la clôture algébrique de K .

D'où le degré de α , nombre de ces images distinctes.

Bien entendu, on peut remplacer la clôture algébrique par toute extension normale de K contenant L .

EXTENSION

La trace d'un

Une extension finie de K est dite *extension normale* si elle est le corps de rupture d'un polynôme séparable sur K . Une extension finie L de K est dite *extension normale* si elle est le corps de rupture d'un polynôme séparable sur K . Une extension finie L de K est dite *extension normale* si elle est le corps de rupture d'un polynôme séparable sur K . Une extension finie L de K est dite *extension normale* si elle est le corps de rupture d'un polynôme séparable sur K .

- Le calcul de la trace de x dans L est noté $T(x)$. Si $L = K(x)$, on a $T(x) = x$.

est le polynôme

son image par

et la diagonale de x^n sur x^{n-1} . On a montré

La trace est sur) et c'est ce tout court, sans dans le contexte

- Si l'on se base sur la base $(y_1, \dots, y_n)$ de L sur K , on a $y_i x^{j-1}$ dont $j = n - 1$.

On en déduit

- Si l'extension est normale, c'est-à-dire la

est formée de

La trace d'un élément algébrique.

Une extension L de degré fini du corps K est en particulier un K -espace de dimension finie et, pour tout $x \in L$, la multiplication par x est une transformation K -linéaire de ce K -espace. Elle possède donc une trace, somme de la diagonale de la matrice représentant la transformation dans une base arbitraire. On l'appelle **trace** de x dans L , et on la note $T_{L|K}(x)$, ou $T_L(x)$ si la précision est superflue, ou même $T(x)$ si les deux corps L et K sont assez clairs dans le contexte.

• Le calcul le plus facile est la trace de x dans l'extension « la plus simple » qui la contient, c'est-à-dire dans $K(x)$.

Si

$$M_x = a_0 + a_1X + \dots + a_{n-1}X^{n-1} + X^n$$

est le polynôme minimum de x , une base de $K(x)$ est

$$(1, x, \dots, x^{n-1})$$

son image par la multiplication par x est

$$(x, x^2, \dots, x^n)$$

et la diagonale de la matrice est nulle, sauf le dernier terme qui est la coordonnée de x^n sur x^{n-1} , soit $-a_{n-1}$.

On a montré

$$T_{K(x)}(x) = -a_{n-1}.$$

La trace est ici la somme de *tous* les conjugués de x (chacun pris une fois bien sûr) et c'est *cette* trace que l'on sous-entend quand on dit « la trace de x sur K » tout court, sans préciser dans quel cadre on se place (sauf si ledit cadre est clair dans le contexte...).

• Si l'on se place dans une extension de degré fini L contenant x , on prend une base $(y_1, \dots, y_p)$ de L sur $K(x)$, d'où une base de L sur K donnée par les $y_i x^j$, avec $i = 1, \dots, p$ et $j = 0, \dots, n-1$. L'image de $y_i x^j$ par la multiplication par x est $y_i x^{j+1}$ dont la coordonnée sur $y_i x^j$ est 0 pour $j \neq n-1$ et $-a_{n-1}$ pour $j = n-1$.

On en déduit que la trace vaut $-pa_{n-1}$, ce qui s'écrit

$$T_L(x) = (L : K(x)) T_{K(x)}(x).$$

• Si l'extension L est normale, alors la famille des conjugués de x par rapport à L , c'est-à-dire la famille

$$(\sigma(x))_{\sigma \in G(L|K)}$$

est formée des conjugués de x chacun répété p fois.

Dans un corps de rupture, la trace d'un élément est la somme de la famille de ses images par le groupe de Galois.

En particulier, la trace est additive : la trace d'une somme est la somme des traces.

- Dans le cas de $\mathbb{C}$ sur $\mathbb{R}$, la trace de $x = a + bi$ est $2a$, même si b est nul : dans ce dernier cas a est réel, mais on le compte deux fois car le degré de $\mathbb{C}$ sur $\mathbb{R}$ est 2.

- Si un élément a une trace nulle dans une extension, il en est de même dans toute extension.

C'est le cas par exemple d'un radical d'ordre *premier* p d'un élément de K qui n'a pas de racine p -ième dans K : le polynôme minimum est alors $X^p - a$.

- L'élément j est racine cubique de 1, mais sa trace sur $\mathbb{Q}$ est -1 .

- L'élément $1 + i$ est racine quatrième de -4 , mais sa trace sur $\mathbb{Q}$ est $+2$ car son polynôme minimum est $X^2 - 2X + 2$.

- Pour p premier la trace d'une racine primitive p -ième de l'unité est -1 .

- Si n n'est pas premier la trace d'une racine primitive n -ième de l'unité peut être nulle (c'est le cas pour $n = 4, 8, 9, 12$) ou égale à $+1$ (exemple : $n = 6, 10$).

- si l'extension
- la n
- si p est égale

Exercice

1. Te le O
2. Si de Q
3. So ég

M

Si

et

4. O es

Si es
It p

o

5. E n E d n z d

La norme d'un élément algébrique.

Dans les mêmes conditions (extension L de degré fini sur K), la multiplication par x dans L possède un déterminant. On l'appelle **norme** de x dans L , et on la note $N_{L,K}(x)$, ou $N_L(x)$, ou $N(x)$ si les précisions sont superflues.

On prouve de manière analogue (en appelant $M_x = a_0 + a_1X + \dots + X^n$ le polynôme minimum de x sur K) :

- la norme de x dans $K(x)$ est $(-1)^n a_0$;
- si l'on se place dans une extension L de $K(x)$, la norme est élevée à la puissance $L : K(x)$

$$N_L(x) = (N_{K(x)}(x))^{(L : K(x))};$$

- la norme d'un élément de K est cet élément élevé à la puissance $L : K$;
- si l'extension L est normale, la norme de x dans L est égale au produit des images de x par le groupe de Galois (c'est donc le produit de la famille des conjugués de x);
- la norme est multiplicative

$$N_L(xy) = N_L(x)N_L(y)$$

(au moins si L est extension normale);

- dans une extension quadratique $K(u)$, la norme de $a + bu$ est $a^2 - u^2b^2$.

st la somme des

est $2a$, même si b
compte deux fois

ision, il en est de

premier p d'un
 K : le polynôme

de sur $\mathbb{Q}$ est -1 .

mais sa trace sur
 $-2X + 2$.

n -ième de l'unité

primitive n -ième de
 $9, 12$ ou égale à

a multiplication
dans L , et on la
es.

$X + \dots + X^n$ le

z est élevée à la

issance $L : K$;
e au produit des
de la famille des

t est $a^2 - u^2b^2$.

- si la norme de $x \in L$ sur K est égale à 1, elle reste égale à 1 dans toute extension de L . C'est le cas des racines primitives p -ièmes de l'unité (p premier);
- la norme de toute racine de l'unité est 1 ou -1 ;
- si p est premier et si $a \in K$ n'a pas de racine p -ième dans K , la norme de $\sqrt[p]{a}$ est égale à a (on suppose $p \neq 2$).

Exercices

1. Tout groupe fini est le groupe de Galois d'une certaine extension de $\mathbb{Q}$ (on utilisera le fait qu'un groupe fini est sous-groupe d'un groupe symétrique).
On ne sait pas si l'on peut exiger que l'extension soit normale...
2. Si une extension n'est pas normale, la trace est-elle encore la somme de la famille des images par le groupe de Galois ? Donner des exemples.
Question analogue pour la norme.
3. Soit K_1 et K_2 des extensions de K (dans une clôture algébrique donnée). Une égalité analogue à celle liant le P.P.C.M. et le P.G.C.D. de deux entiers serait

$$(K_1 K_2 : K) (K_1 \cap K_2 : K) = (K_1 : K) (K_2 : K).$$

Montrer qu'elle peut être fausse, en étudiant

$$K_1 = \mathbb{Q}(\sqrt[3]{2}) \quad \text{et} \quad K_2 = \mathbb{Q}(j\sqrt[3]{2}).$$

Si l'on suppose que K_1 et K_2 sont extensions normales de K , on vérifiera l'égalité

$$G(K_1 K_2 | K_1 \cap K_2) = G(K_1 | K_1 \cap K_2) \times G(K_2 | K_1 \cap K_2)$$

et on en déduira que l'égalité ci-dessus est vraie.

4. On suppose que le groupe de Galois d'une extension normale de degré fini L sur K est cyclique.

Si σ est un générateur de $G(L|K)$, vérifier que, pour tout $x \in L$, l'élément $x - \sigma(x)$ est de trace nulle.

Inversement, si $y \in L$ est de trace nulle, existe-t-il $x \in L$ avec $y = x - \sigma(x)$? On pourra considérer un élément z de trace non nulle, et l'élément x donné par

$$T(z)x = y\sigma(z) + (y + \sigma(y))\sigma^2(z) + \dots + (y + \sigma(y) + \dots + \sigma^{n-2}(y))\sigma^{n-1}(z)$$

où n est le degré de L sur K .

5. De manière analogue, l'élément $x(\sigma(x))^{-1}$ est de norme égale à un. Tout élément de norme un est-il de cette forme ?

En utilisant cette réciproque, on montrera que si L est une extension normale de degré n de K dont le groupe de Galois est cyclique, et si L contient les racines n -ièmes de l'unité, alors L est une extension de K par un radical : il existe $z \in L$ avec $z^n \in K$ et $L = K(z)$. On examinera pour cela la norme d'une racine primitive n -ième de l'unité.

6. Une extension algébrique L de K est normale sur K si, et seulement si, tout K -homomorphisme de L dans la clôture algébrique de K (qui contient L) est un K -automorphisme de L .

C'est aussi le corps de rupture d'une famille de polynômes.

7. Dans la chaîne de corps $K_1 \subset K_2 \subset K_3$, K_3 est normale sur K_2 dès qu'elle l'est sur K_1 , mais elle peut être normale sur K_2 sans l'être sur K_1 . On vérifiera ainsi :

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[3]{2}) \quad \text{et} \quad \mathbb{Q} \not\subset \mathbb{Q}(\sqrt[3]{2}).$$

8. Dans la clôture algébrique $\bar{K}$ de K , soient L_1 et L_2 deux extensions normales.

Montrer que l'intersection $L_1 \cap L_2$ est aussi normale, ainsi que le corps $L_1 L_2$ engendré par L_1 et L_2 .

Le groupe de Galois de $L_1 L_2$ sur K est sous-groupe du produit cartésien

$$G(L_1|K) \times G(L_2|K).$$

Montrer qu'il y a égalité dès que $L_1 \cap L_2$ est égal à K . Est-ce nécessaire ?

9. Soit K une extension normale de k . On se place dans une clôture algébrique de k , on prend une extension arbitraire L de k .

Vérifier

$$L \subset KL, \quad K \cap L \subset K, \quad G(KL|L) = G(K|K \cap L).$$

Montrer que $KL : L$ divise $K : k$. Étudier l'exemple

$$k = \mathbb{Q}, \quad K = \mathbb{Q}(j\sqrt[3]{2}) \quad \text{et} \quad L = \mathbb{Q}(\sqrt[3]{2})$$

pour constater que ce dernier résultat est faux sans l'hypothèse de normalité de K sur k .

10. Si, dans la suite de corps $K \subset H \subset L$, les extensions L et H de K sont normales (éventuellement de degré fini), le groupe de Galois de H sur K est le quotient de celui de L sur K par celui de L sur H .

Que reste-t-il si l'on élimine une des hypothèses de normalité ?

Gru

Comme
il y a de re
de Galois
permutati

Le plus
toutes les
rationnell
« concrets
générale, c
On peut e
racines de
seront bo
symétriqu

La position

Partons
d'une fami
éléments a

des fractio

Notre p

est Σ_n tout
les permu
rationnell

La clé d
sont algéb
fonctions.

D'UN POLYNÔME

et seulement si, tout (qui contient L) est un

s.

sur K_2 dès qu'elle l'est K_1 . On vérifiera ainsi :

$(\sqrt[4]{2})$.

extensions normales.

nsi que le corps $L_1 L_2$

roduit cartésien

st-ce nécessaire ?

ure algébrique de k , on

$[K \cap L)$.

$(\sqrt{2})$

èse de normalité de K

f de K sont normales
r K est le quotient de

lité ?

Groupe de Galois de l'équation générale

Comme on a pu s'en rendre compte sur les quelques exemples précédents, plus il y a de relations rationnelles entre les racines sur le corps de base plus le groupe de Galois d'un polynôme est petit, puisque les conditions imposées aux bonnes permutations sont plus fortes.

Le plus gros groupe de Galois possible est le groupe symétrique, ou groupe de toutes les permutations des racines. C'est ce qui arrive quand les seules relations rationnelles entre les racines sont les relations symétriques. Il y a beaucoup de cas « concrets », mais le cas qui paraît le plus favorable est celui de l'équation générale, c'est-à-dire le cas où les coefficients sont algébriquement indépendants. On peut espérer qu'il y aura le moins possible de relations rationnelles entre les racines de l'équation générale : dans ces conditions toutes les permutations seront bonnes. Bien entendu, « le moins possible » signifie « seulement les symétriques ».

La position du problème.

Partons d'un corps K (qui sera souvent le corps $\mathbb{Q}$ ou un corps le contenant) et d'une famille de n indéterminées sur K , soit $(a_0, a_1, \dots, a_{n-1})$: ce sont donc des éléments algébriquement indépendants sur K qui engendrent le corps

$$K(a_0, a_1, \dots, a_{n-1}) = K_n$$

des fractions rationnelles à n indéterminées sur K .

Notre propos est de montrer que le groupe de Galois du polynôme

$$X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0 \in K_n[X]$$

est Σ_n tout entier (sur le corps de base K_n bien sûr), ce qui revient à dire que toutes les permutations des racines $(x_1, x_2, \dots, x_n)$ conservent toutes les relations rationnelles entre ces racines sur K_n .

Et il y a de telles relations rationnelles, ne serait-ce que celles que l'on a déjà vues, du genre

$$x_1 + \dots + x_n + a_{n-1} = 0 \quad \text{ou} \quad x_1 \dots x_n - (-1)^n a_0 = 0.$$

La clé de la démonstration réside dans les deux faits suivants : les racines x_i sont algébriquement indépendantes sur K et les a_i en sont, au signe près, les fonctions symétriques élémentaires.

En fait, on va démontrer successivement :

- le groupe de Galois du corps de toutes les fractions rationnelles sur le sous-corps des fractions rationnelles symétriques est le groupe symétrique Σ_n ;
- les racines $(x_1, \dots, x_n)$ ne vérifient aucune relation rationnelle sur K (pas sur le corps de base K_n bien sûr...).

Le résultat s'en déduira, les indéterminées X_i jouant le rôle des racines du polynôme et les polynômes symétriques élémentaires celui des coefficients de ce polynôme.

Les fractions rationnelles symétriques.

On a montré directement que toute fraction rationnelle symétrique s'exprimait rationnellement à l'aide des n suivantes (voir p. 39) :

$$\sigma_1 = X_1 + \dots + X_n$$

$$\sigma_2 = \sum_{i < j} X_i X_j$$

.....

$$\sigma_p = \sum_{1 \leq i_1 < \dots < i_p \leq n} X_{i_1} \dots X_{i_p}$$

.....

$$\sigma_n = X_1 \dots X_n$$

Autrement dit, si

$$K_s(X_1, \dots, X_n)$$

est le corps des fractions rationnelles symétriques, la première inclusion de la chaîne évidente

$$K(\sigma_1, \dots, \sigma_n) \subset K_s(X_1, \dots, X_n) \subset K(X_1, \dots, X_n)$$

est une égalité.

On peut retrouver ce résultat (et d'autres dont on se servira ici) en vérifiant simplement que $K(X_1, \dots, X_n)$ a même degré sur ses deux sous-corps emboîtés

$$K(\sigma_1, \dots, \sigma_n) \quad \text{et} \quad K_s(X_1, \dots, X_n).$$

La remarque essentielle est alors : les X_i sont exactement les racines de

$$T = X^n - \sigma_1 X^{n-1} + \dots + (-1)^n \sigma_n \in K(\sigma_1, \dots, \sigma_n)[X]$$

donc $K(X_1, \dots, X_n)$ est le corps de rupture de T sur $K(\sigma_1, \dots, \sigma_n)$ et *a fortiori* sur $K_s(X_1, \dots, X_n)$.

Mais toute permutation des racines de T laisse fixe aussi bien $K(\sigma_1, \dots, \sigma_n)$ que $K_s(X_1, \dots, X_n)$. Ceci s'écrit

$$G(K(X_1, \dots, X_n) | K(\sigma_1, \dots, \sigma_n)) = G(K(X_1, \dots, X_n) | K_s(X_1, \dots, X_n)) = \Sigma_n$$

Or l'ordre

$$K(X_1, \dots$$

Conséque

- $K(\sigma_1, \dots$
- « artisanale
- la vale
- symétrique
- pour to
- le corps de
- si $(z_1, \dots$
- corresponde
- fixes leurs fc

L'indépenda

Revenons

où les coeffi

comme des
Le groupe
sera le group
précédent. T
indépendan
 $K(X_1, \dots, X$
et les a_i son

Raisonne
entre les rac
vérifiant

L'idée est
polynômes
polynômes r
symétrique S

Or, le pol
soit

où R est un
Si l'on rer

nelles sur le sous-
métrique Σ_n ;

nelle sur K (pas sur

de des racines du
coefficients de ce

nelle symétrique
39) :

ère inclusion de la

, X_n)

vira ici) en vérifiant
ous-corps emboîtés

t les racines de

, σ_n) [X]

, σ_n) et *a fortiori*

bien $K(\sigma_1, \dots, \sigma_n)$

$X_1, \dots, X_n) = \Sigma_n$

Or l'ordre du groupe de Galois est le degré de l'extension. D'où

$$K(X_1, \dots, X_n) : K(\sigma_1, \dots, \sigma_n) = K(X_1, \dots, X_n) : K_s(X_1, \dots, X_n) = n !$$

Conséquences :

- $K(\sigma_1, \dots, \sigma_n) = K_s(X_1, \dots, X_n)$, ce que l'on avait montré de manière plus « artisanale » (voir p. 39);
- la valeur, sur les racines d'un polynôme, d'une fraction rationnelle symétrique est dans le corps engendré par les coefficients;
- pour tout n , il existe un corps et un polynôme de degré n sur ce corps tel que le corps de rupture soit de degré $n !$ (donc le plus grand possible);
- si $(z_1, \dots, z_n)$ sont algébriquement indépendants sur K , leurs permutations correspondent exactement aux K -automorphismes de $K(z_1, \dots, z_n)$ laissant fixes leurs fonctions symétriques élémentaires.

L'indépendance algébrique des racines de l'équation générale.

Revenons à notre polynôme

$$P = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0$$

où les coefficients a_i sont algébriquement indépendants (donc se comportent comme des indéterminées) sur le corps K . Appelons $x_1, \dots, x_n$ les racines.

Le groupe de Galois de ce polynôme sur le corps engendré par les coefficients sera le groupe symétrique Σ_n tout entier si l'on montre que l'on se ramène au cas précédent. Tout revient à prouver que la famille $(x_1, \dots, x_n)$ est algébriquement indépendante sur K . En effet, on se trouve alors en présence du corps de rupture $K(x_1, \dots, x_n)$ et du corps de base $K(a_0, \dots, a_n)$ où les x_i sont des indéterminées et les a_i sont, au signe près, leurs fonctions symétriques élémentaires.

Raisonnons par l'absurde, en supposant qu'il existe une relation rationnelle entre les racines, c'est-à-dire un polynôme T à n indéterminées sur K , non nul, vérifiant

$$T(x_1, \dots, x_n) = 0.$$

L'idée est toujours de « symétriser » : au polynôme T on associe les $n !$ polynômes déduits par permutations des indéterminées. Aucun de ces polynômes n'est nul, leur produit S non plus. Mais ce produit est un polynôme symétrique S , non nul, vérifiant encore

$$S(x_1, \dots, x_n) = 0.$$

Or, le polynôme S s'exprime à l'aide des polynômes symétriques élémentaires, soit

$$S(X_1, \dots, X_n) = R(\sigma_1, \dots, \sigma_n)$$

où R est une fraction rationnelle non nulle.

Si l'on remplace les indéterminées X_i par les racines x_i de P , il reste

$$0 = R(-a_{n-1}, a_{n-2}, \dots, (-1)^n a_n).$$

Comme R est non nul, c'est là une relation de dépendance rationnelle sur K entre les a_i , ce qui contredit le fait que les a_i sont algébriquement indépendants sur K .
On peut énoncer (en mettant à part le coefficient dominant du polynôme).

Si la famille des coefficients est algébriquement indépendante, il en est de même de la famille des racines.

Attention : il faut la famille de *tous* les coefficients (sauf le dominant bien sûr).

- Si p et q sont des indéterminées sur $\mathbb{Q}$, les coefficients de

$$X^3 + pX + q \in \mathbb{Q}(p, q)(X)$$

forment la famille $(0, p, q)$, qui est algébriquement dépendante ; et d'ailleurs, les racines x_1, x_2, x_3 vérifient la relation de dépendance

$$x_1 + x_2 + x_3 = 0.$$

- Si l'on prend le polynôme

$$X^3 + \pi X^2 + eX + e^* \in \mathbb{C}[X],$$

les coefficients sont algébriquement indépendants sur $\mathbb{Q}$ (mais pas sur $\mathbb{R}$), il en sera donc de même des racines.

- On prendra bien garde que les racines de l'équation générale sont algébriquement indépendantes sur K , mais pas sur le corps $K(a_0, a_1, \dots, a_{n-1})$ engendré par les coefficients (ne serait-ce qu'à cause de leur somme égale à $-a_{n-1}$).

Le groupe de Galois de l'équation générale.

Une conséquence immédiate concerne le groupe de Galois de

$$X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0$$

sur le corps $K(a_0, a_1, \dots, a_{n-1})$ des fractions rationnelles à n indéterminées. On l'énoncera :

Le groupe de Galois de l'équation générale de degré n est le groupe Σ_n de toutes les permutations des racines.

Autrement dit, toute relation rationnelle entre les racines x_i , sur le corps de base $K_n = K(a_0, a_1, \dots, a_{n-1})$, est de la forme

$$R(x_1, \dots, x_n) = y$$

où y est dans K_n et R est une fraction rationnelle *symétrique* à n indéterminées sur K_n .

Exercice

1. Ch

po

2. En

s_2

3. Si l
cet
coe
rés

4. Sur
leu

nnelle sur K entre
épendants sur K.
t du polynôme).

ndépendante, il en

minant bien sûr).

coefficients de

ment dépendante;
t la relation de

ints sur $\mathbb{Q}$ (mais
es.

quation générale
s pas sur le corps
nts (ne serait-ce

de

déterminées. On

,ré n est le groupe

. sur le corps de

n indéterminées

Exercices.

1. Chercher une fraction rationnelle symétrique T vérifiant

$$T(X_1 + a, \dots, X_n + a) = T(X_1, \dots, X_n)$$

pour un certain a dans le corps de base.

2. En appelant s_p la somme des puissances p -ièmes des racines, vérifier

$$s_1 = s_2 = \dots = s_{n-1} = 0 \quad \text{pour le polynôme } X^n - a$$

$$s_2 = s_3 = \dots = s_n = 0 \quad \text{pour } X^n - aX^{n-1} + \frac{a^2}{2!}X^{n-2} + \dots + (-1)^n \frac{a^n}{n!}.$$

3. Si les racines d'une équation sont algébriquement indépendantes sur un corps K , cette équation est-elle l'équation générale sur K ? (Il faut donc examiner si les coefficients sont algébriquement indépendants sur K , c'est la réciproque d'un des résultats du chapitre).
4. Sur un corps K , n éléments sont algébriquement indépendants si, et seulement si, leurs n fonctions symétriques élémentaires le sont.

L'utilisation des groupes de Galois

Le groupe de Galois d'un polynôme s'avère être un outil particulièrement puissant pour répondre à certaines questions. On va voir en particulier comment il donne la réponse aux « problèmes historiques » posés au début.

Le point essentiel sera la correspondance qui s'établit entre les sous-groupes du groupe de Galois et les extensions du corps de base.

Répétons que, dans tout ce qui suit, on ne s'occupera pas des problèmes de caractéristiques : s'il le faut, on supposera que l'on est en caractéristique nulle, donc que les corps contiennent tous $\mathbb{Q}$.

Réduire le groupe de Galois

Quand on a étudié ce que signifie « résoudre une équation », on a vu qu'il s'agissait de passer du corps de base à un corps contenant les racines, et ceci par adjonctions successives de radicaux (voir p. 22).

D'où l'idée de voir comment varie le groupe de Galois quand on adjoint un ou plusieurs éléments algébriques au corps de base.

La notion de réduction.

Si l'on augmente le corps de base, il y a *plus* de relations rationnelles possibles entre les racines d'un polynôme, donc il y a *moins* de bonnes permutations et il est logique d'en déduire que l'on diminue ainsi le groupe de Galois.

Soyons plus précis. On part d'un polynôme $P \in K[X]$, dont les racines (dans la clôture algébrique de K par exemple) sont $(x_1, \dots, x_n)$; le corps de rupture de P sur K est $K(x_1, \dots, x_n)$.

Prenons maintenant une extension (en général algébrique) H de K ; le corps de rupture de P sur H sera $H(x_1, \dots, x_n)$.

Le polynôme P possède

- un groupe de Galois sur K , soit $G(P|K)$, formé des K -automorphismes de $K(x_1, \dots, x_n)$;
- un groupe de Galois sur H , soit $G(P|H)$, formé des H -automorphismes de $H(x_1, \dots, x_n)$.

D'après les remarques initiales, le second devrait être contenu dans le premier. Il est facile de montrer qu'effectivement $G(P|H)$ est un sous-groupe de $G(P|K)$.

En voyant les groupes de Galois comme groupes de permutations des racines, c'est clair : toute bonne permutation des x_i par rapport à H est bonne *a fortiori* par rapport à son sous-corps K , car toute relation rationnelle sur K est une relation rationnelle sur H , donc est respectée par ladite permutation.

Si l'on préfère le point de vue des automorphismes, on vérifie aisément qu'un H -automorphisme de $H(x_1, \dots, x_n)$ laisse fixe K et permute les x_i , donc laisse $K(x_1, \dots, x_n)$ invariant; sa restriction à $K(x_1, \dots, x_n)$ est bien un K -automorphisme de ce dernier, et l'application « restriction » est un homomorphisme injectif de groupes de $G(H(x_1, \dots, x_n)|H)$ dans $G(K(x_1, \dots, x_n)|K)$.

Réduction

Le cas le simple, c'est : Galois de F sous-groupe ou non au

• Si l'on irrationnell $K(\theta)$ peut grand : l'ac

En augmentant le corps de base, on dit que l'on a **réduit** le groupe de Galois à un sous-groupe.

Le groupe de Galois de $X^4 - 2$ sur $\mathbb{Q}$ est d'ordre 8 (on l'a appelé groupe diédral D_8), le corps de rupture étant $\mathbb{Q}(\sqrt[4]{2}, i)$.

- Si l'on prend $K_1 = \mathbb{Q}(\sqrt{2})$ comme corps de base, on impose que $\sqrt{2}$ soit fixe, ce qui exige que l'image de $\sqrt[4]{2}$ soit elle ou son opposée (et non plus $i\sqrt[4]{2}$ ou $-i\sqrt[4]{2}$), donc le groupe de Galois sur K_1 est d'ordre 4, c'est

$$G(K_1(\sqrt[4]{2}, i)|K_1) = C_2 \times C_2.$$

- On peut augmenter encore en passant à $K_2 = \mathbb{Q}(\sqrt[4]{2})$. Cette fois, $\sqrt[4]{2}$ est fixe, donc tout ce que l'on peut faire est transformer i en i ou $-i$, d'où un groupe de Galois d'ordre 2, formé de l'identité et la conjugaison complexe :

$$G(K_2(i)|K_2) = C_2.$$

- Enfin, sur $K_3 = \mathbb{Q}(\sqrt[4]{2}, i)$, le groupe de Galois est réduit à l'identité : à la chaîne de corps

$$\mathbb{Q} \subset K_1 \subset K_2 \subset K_3$$

correspond la chaîne des groupes de Galois de $X^4 - 2$

$$D_8 \supset C_2 \times C_2 \supset C_2 \supset \text{id}.$$

On reviendra sur cette « correspondance de Galois ».

Réduction du groupe par adjonction d'un élément au corps.

Le cas le plus naturel est celui qui consiste à passer d'un corps à une extension simple, c'est-à-dire à adjoindre un élément algébrique : que dire du groupe de Galois de $P \in K[X]$ sur $K(\theta)$ par rapport à son groupe de Galois sur K ? C'est un sous-groupe, mais encore ?

Comme on peut s'y attendre, le résultat est différent suivant que θ appartient ou non au « cadre naturel » de P , c'est-à-dire au corps de rupture de P .

- Si l'on adjoint à K un élément θ hors du corps de rupture de P (on disait une **irrationnelle accessoire** dans les vieux manuels), alors le corps de rupture de P sur $K(\theta)$ peut être le même que celui sur K , bien que le corps soit strictement plus grand : l'adjonction d'une irrationnelle accessoire peut ne rien réduire du tout...

- Ainsi, le corps de rupture de $X^2 + 1$ sur $\mathbb{Q}$ est $\mathbb{Q}(i)$, il ne contient pas j , mais l'adjonction de j ne change pas le groupe de Galois :

$$G(X^2 + 1|\mathbb{Q}) = G(X^2 + 1|\mathbb{Q}(j)) = C_2.$$

- Mais $x = \frac{1+i}{\sqrt{2}}$ n'est pas non plus dans le corps de rupture, et pourtant l'adjonction de cette irrationnelle accessoire réduit strictement le groupe de Galois, puisque son carré est i , racine de $X^2 + 1$: le corps $\mathbb{Q}(x)$ contient le corps de rupture de $X^2 + 1$, ce qui donne

$$G\left(X^2 + 1 \mid \mathbb{Q}\left(\frac{1+i}{\sqrt{2}}\right)\right) = \text{id.}$$

- De même, $\sqrt[4]{2}$ est une irrationnelle accessoire de $X^2 - 2$ pour $\mathbb{Q}$, car hors du corps de rupture $\mathbb{Q}(\sqrt{2})$, mais son adjonction réduit le groupe de Galois de C_2 à id.
- Le calcul $(i + \sqrt{3})^3 - 8(i + \sqrt{3}) = -8\sqrt{3}$ montre que l'adjonction à $\mathbb{Q}$ de l'irrationnelle accessoire $i + \sqrt{3}$ au corps de rupture $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ de $(X^2 - 2)(X^2 - 3)$ réduit le groupe (qui est d'ordre 4) à un sous-groupe d'ordre 2.

• Plus intéressant est ce qui se passe quand on adjoint une **irrationnelle naturelle**, c'est-à-dire un élément du corps de rupture (donc une fonction rationnelle des racines du polynôme).

Appelons $(x_1, \dots, x_n)$ les racines de $P \in K[X]$, et θ un élément du corps de rupture $K(x_1, \dots, x_n)$ de P sur K . Alors, et contrairement au cas d'une irrationnelle accessoire, le corps de rupture de P sur $K(\theta)$ est *encore* $K(x_1, \dots, x_n)$, puisque θ est dans ce dernier corps.

Dès lors, l'ordre du groupe de Galois $G(P|K)$ est le degré de $K(x_1, \dots, x_n)$ sur K , alors que l'ordre de son sous-groupe $G(P|K(\theta))$ est le degré de $K(x_1, \dots, x_n)$ sur $K(\theta)$. Le quotient de ces deux ordres est le degré de $K(\theta)$ sur K , donc le degré de l'irrationnelle naturelle θ sur K .

Par définition, l'indice d'un sous-groupe est le quotient de l'ordre du groupe par celui du sous-groupe. On a montré :

L'adjonction d'un élément de degré m du corps de rupture réduit le groupe de Galois à un sous-groupe d'indice m .

En particulier, la réduction du groupe de Galois sera stricte si l'on adjoint un élément du corps de rupture qui soit hors du corps de base. En adjoignant au corps de base une fonction rationnelle des racines, on aura donc intérêt en tout cas à prendre une fonction rationnelle non symétrique. Tout ceci traduit la méthode de Lagrange, adjonction successive des $T_i(x_1, \dots, x_n)$ (voir p. 180).

On n'oubliera pas que le degré d'un élément θ est le nombre de ses conjugués.

Une dernière remarque : si on l'adjoint à K deux irrationnelles naturelles θ et θ' , le groupe de Galois de P sur $K(\theta, \theta')$ est l'intersection des groupes de Galois de P sur $K(\theta)$ et sur $K(\theta')$

$$G(P|K(\theta, \theta')) = G(P|K(\theta)) \cap G(P|K(\theta')).$$

Quelques exemples.

1° Le groupe de Galois de $X^4 - 2$ sur $\mathbb{Q}$ est d'ordre 8, le corps de rupture contient $\sqrt{2}$ qui est de degré 2 sur $\mathbb{Q}$, donc le groupe de Galois de $X^4 - 2$ sur $\mathbb{Q}(\sqrt{2})$ doit être d'indice 2, c'est-à-dire d'ordre 4. On l'a vérifié ci-dessus.

2° Si x est une racine du polynôme P , irréductible de degré n sur K , alors l'adjonction de x réduit le groupe de Galois à un sous-groupe d'indice n (puisque P est le polynôme minimum de x sur K) : l'ordre de $G(P|K)$ est n fois l'ordre de $G(P|K(x))$.

3° Dans le cours de la résolution de l'équation de degré 3 (voir p. 57), on a introduit l'élément

$$\alpha = (x_1 + x_2j + x_3j^2)^3.$$

Plus précisément, on partait de

$$X^3 + pX + q \in K[X]$$

et on commençait par adjoindre j à K (on supposera ici que K contient déjà j). Dans ces conditions, si x_1, x_2, x_3 sont les racines, l'élément α est dans le corps de rupture de P sur K et ne prend que deux valeurs distinctes au plus par *tout* le groupe des permutations de (x_1, x_2, x_3) : ce sont

$$\alpha = (x_1 + x_2j + x_3j^2)^3 \quad \text{et} \quad \beta = (x_1 + x_3j + x_2j^2)^3.$$

Comme le groupe de Galois est sous-groupe de Σ_3 , α est de degré 2 au plus. D'ailleurs, α et β sont les racines de

$$X^2 + 27qX - 27p^3$$

dont le discriminant est $9 \times (-3)(-4p^3 - 27q^2)$. Or 9 et -3 sont des carrés dans K (-3 est le carré de $1 + 2j$), donc tout dépend de $\Delta = -4p^3 - 27q^2$ (encore lui...).

• $\sqrt{\Delta} \in K$: les éléments α et β sont dans K , et leur adjonction n'avance à rien.

D'autre part, ils ne sont égaux que si Δ est nul (ce qui signifie que $X^3 + pX + q$ a une racine multiple), et dans le cas contraire ils ne sont pas conjugués. Comme on passe de α à β en échangeant deux des trois indices, le groupe de Galois ne comprend aucune transposition : c'est soit le groupe alterné A_3 , soit seulement l'identité.

• $\sqrt{\Delta} \notin K$: ici, α est d'ordre 2 sur K , son conjugué étant β , et l'adjonction de α à K réduit le groupe de Galois à un sous-groupe d'indice 2. Dans ces conditions, le groupe de Galois est d'ordre pair, il est égal à Σ_3 tout entier ou formé de l'identité et une transposition.

Bien entendu, si l'on part de l'équation générale, p et q sont des indéterminées, le corps de base K est $\mathbb{Q}(p, q, j)$, et Δ n'est pas un carré dans ce corps.

4° Au degré 4, on partait des racines x_1, x_2, x_3, x_4 de

$$X^4 + aX^2 + bX + c \in K[X]$$

et on introduisait l'irrationnelle naturelle (voir p. 64)

$$\alpha = x_1x_2 + x_3x_4.$$

Si l'on effectue toutes les permutations, on trouve au plus deux autres valeurs, qui sont

$$\begin{aligned}\beta &= x_2x_3 + x_1x_4 \\ \gamma &= x_2x_4 + x_1x_3.\end{aligned}$$

L'élément α est donc de degré inférieur à 3. D'ailleurs, le polynôme de degré 3 nul en α, β, γ est

$$T = X^3 - aX^2 - 4cX + 4ac - b^2.$$

D'où les deux cas :

- si T possède une racine dans K , il est réductible, le degré de α sur K est 2 ou 1 et l'adjonction de α réduit le groupe de Galois à un sous-groupe d'indice 2 ou ne le réduit pas ;
- si T n'a pas de racine dans K , il est irréductible, et T est le polynôme minimum commun de α, β, γ .

L'adjonction de α réduit donc le groupe de Galois à un sous-groupe d'indice 3 et l'ordre du groupe de Galois est un multiple de 3.

C'est, ici encore, ce qui se produit si l'on part de l'équation générale, sur le corps $\mathbb{Q}(a, b, c)$ des fractions rationnelles à trois indéterminées sur $\mathbb{Q}$.

Un exemple plus « concret » :

$$X^4 + X + 1 \in \mathbb{Q}[X]$$

pour lequel on trouve

$$T = X^3 - 4X - 1.$$

Le polynôme est irréductible sur $\mathbb{Q}$, car si p et q étaient des entiers premiers entre eux avec $T\left(\frac{p}{q}\right) = 0$ on trouverait

$$p^3 - 4pq^2 - q^3 = 0$$

ce qui exigerait que p et q se divisent l'un l'autre : or 1 et -1 ne sont pas racines de T .

En conclusion, l'ordre du groupe de Galois de $X^4 + X + 1$ sur $\mathbb{Q}$ est multiple de 3. On le déterminera plus loin (voir p. 225).

Un exemple

Comme l'adjonction d'une racine rationnelle ne change pas le rapport aux autres racines. L'idée la plus simple est symétrique et transpose en prenant une

Partons d'une racine. On

qui est dans K c'est une fois est nul si, et est non nul P.G.C.D. de

Notre irr

qui n'est pas toutes les p seulement si le groupe c équivalent c alors

Dans le c l'équation g l'adjonction le groupe d permutation racines et la

permutation

Traductio

$2, p$ et q sont des
et Δ n'est pas un

$3, x_4$ de

p. 64)

ive au plus deux

3. D'ailleurs, le

4^2 .

ole, le degré de α
oupe de Galois à

tible, et T est le

alois à un sous-
est un multiple

it de l'équation
onnelles à trois

aient des entiers

it

or 1 et -1 ne

$+X-1$ sur $\mathbb{Q}$
voir p. 225).

Un exemple classique : le discriminant.

Comme on l'a signalé, une irrationnelle naturelle (c'est-à-dire une fonction rationnelle des racines) doit, pour être intéressante, ne pas être symétrique par rapport aux racines : sinon elle est dans le corps de base.

L'idée la plus simple est de prendre une fonction non symétrique dont le carré est symétrique : ce sera donc une fonction changeant de signe dès que l'on transpose deux racines. Exemple : le produit des différences des racines, en prenant une seule fois chaque couple.

Partons donc d'un polynôme $P \in K[X]$ et de la famille $(x_1, \dots, x_n)$ de ses racines. On appelle **discriminant** de P l'élément

$$\Delta = \prod_{i < j} (x_i - x_j)^2$$

qui est dans le corps engendré par les coefficients de P (donc *a fortiori* dans K) car c'est une fonction rationnelle symétrique des racines. Notons en passant que Δ est nul si, et seulement si, P a une racine multiple. On supposera s'il le faut que Δ est non nul et alors n est le nombre de racines de P : il suffit de diviser P par le P.G.C.D. de P et P' (voir p. 31).

Notre irrationnelle naturelle sera

$$\alpha = \prod_{i < j} (x_i - x_j)$$

qui n'est pas symétrique par rapport aux racines, car elle change de signe pour toutes les permutations impaires. Elle sera donc dans le corps de base si, et seulement si, les permutations impaires sont toutes mauvaises, ce qui signifie que le groupe de Galois est un sous-groupe du groupe alterné A_n . Il est donc équivalent de dire que les racines carrées de $\Delta \in K$ sont encore dans K . On écrira alors

$$\sqrt{\Delta} \in K \Leftrightarrow G(P|K) \subset A_n.$$

Dans le cas contraire, c'est-à-dire si Δ n'est pas un carré dans K (exemple de l'équation générale), il y a certaines permutations impaires qui sont bonnes et l'adjonction à K de $\sqrt{\Delta}$ réduit le groupe de Galois à un sous-groupe d'indice 2 : le groupe de Galois de P sur l'extension quadratique $K(\sqrt{\Delta})$ est formé des permutations des racines qui conservent les relations rationnelles sur K entre ces racines et laissent fixe l'expression $\prod_{i < j} (x_i - x_j)$, il est donc égal à l'ensemble des permutations paires du groupe de Galois de P sur K .

Traduction : dans tous les cas

$$G(P|K(\sqrt{\Delta})) = G(P|K) \cap A_n.$$

- Le discriminant de $X^3 + pX + q$ est $\Delta = -4p^3 - 27q^2$.

Si p et q sont des indéterminées, le groupe de Galois de ce polynôme sur le corps $\mathbb{Q}(p, q)$ est Σ_3 .

Comme p et q sont encore algébriquement indépendants sur $\mathbb{Q}(j)$, l'adjonction de cette irrationnelle accessoire j ne change pas le groupe de Galois.

Par contre, le groupe de Galois sur $\mathbb{Q}(p, q, j, \sqrt{\Delta})$ est réduit à A_3 , donc toute fonction rationnelle des racines qui a trois valeurs distinctes quand on effectue les trois permutations paires est un élément primitif du corps de rupture sur $\mathbb{Q}(p, q, j, \sqrt{\Delta})$. On peut choisir $x_1 + jx_2 + j^2x_3$.

- Pour l'équation dite bicarrée $X^4 + aX^2 + b$, les racines sont $\pm \sqrt{r_1}$ et $\pm \sqrt{r_2}$, où r_1 et r_2 sont les racines de $X^2 + aX + b$. On trouve alors $\Delta = 16r_1r_2(r_1 - r_2)^4$, soit

$$\Delta = 16b(a^2 - 4b)^2.$$

Le groupe de Galois de $X^4 + aX^2 + b$ est donc contenu dans A_4 si, et seulement si, le corps de base K contient $\sqrt{b}$.

On retrouve les résultats discutés dans le cas irréductible (voir p. 180) : des trois groupes possibles $C_2 \times C_2$, C_4 et D_8 , seul le premier ne contient que des permutations paires.

Le calcul du discriminant de $P \in K[X]$ est assez simple en utilisant le dérivé : en effet, Δ est le résultant de P et P' (voir p. 40) comme on va le voir facilement.

On appelle $(x_1, \dots, x_n)$ la famille des racines de P et a_n son coefficient dominant et l'on écrit

$$\begin{aligned} P(X) &= a_n(X - x_1)(X - x_2) \dots (X - x_n) \\ \text{d'où} \quad P'(x_1) &= a_n(x_1 - x_2)(x_1 - x_3) \dots (x_1 - x_n) \end{aligned}$$

$$\text{puis} \quad P'(x_1)P'(x_2) \dots P'(x_n) = (a_n)^n (-1)^{\frac{n(n-1)}{2}} \prod_{i < j} (x_i - x_j)^2.$$

Si le coefficient dominant vaut 1, on trouve

$$\Delta = (-1)^{\frac{n(n-1)}{2}} P'(x_1)P'(x_2) \dots P'(x_n).$$

Le discriminant est au signe près, le produit des valeurs du dérivé sur la famille des racines du polynôme.

C'est aussi, au signe près, le produit des racines de l'équation transformée de $P(X) = 0$ par $Y = P'(X)$, donc le terme constant de cette équation en Y . On doit

$$\text{multiplier par } (-1)^n \cdot (-1)^{\frac{n(n-1)}{2}} = (-1)^{\frac{n(n+1)}{2}}$$

La nullité de Δ équivaut bien à la nullité d'un des $P'(x_i)$, et le x_i correspondant est racine multiple : satisfaisant pour l'esprit...

La réduction

Les « bc
les noyau:
groupes q

$4p^3 - 27q^2$.
 le Galois de ce
 ndants sur $\mathbb{Q}(j)$,
 e change pas le

est réduit à A_3 ,
 a trois valeurs
 ns paires est un
 $\sqrt{\Delta}$). On peut

les racines sont
 $X^2 + aX + b$.

ontenu dans A_4
 $\sqrt{b}$.
 réductible (voir
 A_4 et D_8 , seul le
 s.

isant le dérivé :
 voir facilement.

son coefficient

$\epsilon_j)^2$.

aleurs du dérivé

transformée de
 n en Y. On doit

correspondant

- Pour $X^3 + pX + q$, on pose $Y = 3X^2 + p$, d'où l'équation

$$X\left(\frac{Y-p}{3} + p\right) = -q$$

qui donne en élevant au carré

$$\frac{Y-p}{3} \left(\frac{Y+2p}{3}\right)^2 - q^2 = 0$$

et le terme constant de $(Y-p)(Y+2p)^2 - 27q^2$ est
 $-4p^3 - 27q^2$.

- Si l'on prend $X^4 + aX + b$, on transforme par $Y = 4X^3 + a$, puis on prend le terme constant, ce qui équivaut à $X^3 = -\frac{a}{4}$. On calcule $X\left(-\frac{a}{4} + a\right) = -b$, puis $-\frac{a}{4} \cdot \left(\frac{3a}{4}\right)^3 = -b^3$, ce qui donne l'expression $\Delta = 256b^3 - 27a^4$ (avec le signe + car $\frac{n(n+1)}{2}$ est pair pour $n = 4$).

- Le polynôme dérivé de $X^n - 1$ est nX^{n-1} , donc le discriminant de $X^n - 1$ est égal à

$$\Delta = (-1)^{\frac{n(n-1)}{2}} n^n p^{n-1}$$

où p est le produit des racines n -ièmes de l'unité.

Or ce produit est le terme constant de $X^n - 1$ multiplié par $(-1)^n$, c'est donc $(-1)^{n-1}$, d'où encore

$$\Delta = (-1)^k n^n$$

$$\text{avec } k = \frac{n(n-1)}{2} + (n-1)^2 = \frac{(n-1)(3n-2)}{2}.$$

Au signe près, on trouve donc, en appelant ω une racine primitive n -ième de l'unité :

$$\prod_{0 \leq i < j < n} (\omega^i - \omega^j)^2 = n^n.$$

La réduction à un sous-groupe normal.

Les « bons » sous-groupes d'un groupe sont les sous-groupes *normaux*, ce sont les noyaux d'homomorphismes de groupes, ceux qui permettent de faire des groupes quotients (voir p. 130).

On écrit $H \triangleleft G$ pour préciser que H est un sous-groupe normal de G , la condition étant la stabilité par les transformations du groupe appelées « conjuguons » :

$$\left. \begin{array}{l} y \in H \\ x \in G \end{array} \right\} \Rightarrow xyx^{-1} \in H.$$

- Tout sous-groupe d'un groupe abélien est normal.
- Le seul sous-groupe normal de Σ_3 autre que lui-même et l'identité est le groupe alterné A_3 . Les trois autres sous-groupes, formés de l'identité et une transposition, ne sont pas normaux : l'égalité

$$(1\ 3)(1\ 2)(1\ 3)^{-1} = (2\ 3)$$

montre que le sous-groupe $H = \{\text{id}, (1\ 2)\}$ ne vérifie pas la condition ci-dessus.

Dès lors, si l'on part d'un polynôme P sur un corps K et si l'on augmente le corps de base, le groupe de Galois est réduit à un sous-groupe : il est naturel de se demander si ce sous-groupe est *normal*.

Ce n'est pas toujours le cas...

Ainsi, si $u = \sqrt[3]{2}$ est la racine cubique réelle de 2, le groupe de Galois de $X^3 - 2$, qui est Σ_3 tout entier sur $\mathbb{Q}$, est réduit sur $\mathbb{Q}(u)$ à un sous-groupe d'indice 3 (car u est de degré 3 sur $\mathbb{Q}$), donc d'ordre 2 ; ce sous-groupe est formé de l'identité et de l'échange des deux racines non réelles, il n'est *pas* normal dans Σ_3 comme on l'a signalé ci-dessus.

Pour y voir plus clair, on va se borner au cas où l'on adjoint des irrationnelles naturelles : on augmente le corps de base tout en restant dans le corps de rupture.

Si $(x_1, \dots, x_n)$ sont les racines de P , on appelle donc L un corps intermédiaire entre le corps de base K et le corps de rupture $K(x_1, \dots, x_n)$, c'est-à-dire

$$K \subset L \subset K(x_1, \dots, x_n).$$

Le sous-groupe $G(P|L) = G(K(x_1, \dots, x_n)|L)$ du groupe

$$G(P|K) = G(K(x_1, \dots, x_n)|K)$$

est-il normal ? Il le sera si l'on peut définir sur le second un homomorphisme de groupes dont le noyau soit exactement le premier.

Or, $G(P|K)$ est le groupe des K -automorphismes de $K(x_1, \dots, x_n)$, et un tel K -automorphisme σ , restreint à L , est un K -automorphisme de L , lequel est l'identité si, et seulement si, L est fixe, c'est-à-dire justement si σ est un L -automorphisme, donc un élément de $G(P|L)$.

En d'autres termes, un candidat naturel d'homomorphisme de noyau $G(P|L)$ est la restriction à L

$$\begin{aligned} \sigma &\rightarrow \sigma|_L \\ G(P|K) &\rightarrow G(L|K). \end{aligned}$$

RÉDUIRE

Mais atten
de $K(x_1, \dots$
transforma

On pour
stable par l
que L est u
 L est satu
conjugués

Si l'on su
me ci-des
 L -automor
C'est donc
 $G(P|K)/G($
Or, cet
prolongear
ment les re
Traducti

Comme
« normal »
groupes : i

Un cas i
 $K(\theta)$ est e
polynôme

De plus,
c'est-à-dire

normal de G , la
groupe appelées

normal.

que lui-même et
tous sous-groupes,
ne sont pas normaux :

ne vérifie pas la

l'on augmente le
il est naturel de se

de 2, le groupe de
est réduit sur $\mathbb{Q}(u)$
degré 3 sur $\mathbb{Q}$, donc
l'ité et de l'échange
al dans Σ_3 comme

t des irrationnelles
le corps de rupture.

corps intermédiaire
(?), c'est-à-dire

homomorphisme de

$x_1, \dots, x_n$), et un tel
me de L , lequel est
ement si σ est un
ne de noyau $G(P|L)$

Mais attention, on a été un peu vite, car cette restriction d'une transformation σ de $K(x_1, \dots, x_n)$ est une application de L dans $K(x_1, \dots, x_n)$ qui sera une transformation de L si, et seulement si, L est stable par σ .

On pourra donc définir l'homomorphisme ci-dessus si, et seulement si, L est stable par le groupe de Galois de P sur K . Pour en être sûr, il suffit de supposer que L est une extension normale de K (c'est-à-dire un corps de rupture), car alors L est saturée par conjugaison et l'image de L par $\sigma \in G(P|K)$ est formée de conjugués d'éléments de L .

Dans l'exemple ci-dessus, L était $\mathbb{Q}(\sqrt[3]{2})$ qui n'est justement pas extension normale de $\mathbb{Q}$.

Si l'on suppose donc que L est extension normale de K , alors l'homomorphisme ci-dessus « restriction à L » a pour noyau le sous-groupe des L -automorphismes de $K(x_1, \dots, x_n)$, c'est-à-dire le groupe de Galois de P sur L . C'est donc là un sous-groupe normal de $G(P|K)$, et le groupe quotient $G(P|K)/G(P|L)$ est isomorphe à l'image de l'homomorphisme.

Or, cet homomorphisme est surjectif, tout K -automorphisme de L se prolongeant en un K -automorphisme de $K(x_1, \dots, x_n)$: on adjoint successivement les racines $x_1, \dots, x_n$ (voir p. 164).

Traduction : le groupe quotient $G(P|K)/G(P|L)$ est $G(L|K)$.

Si l'on augmente le corps de base en une extension normale, tout en restant dans le corps de rupture, le groupe de Galois d'un polynôme est réduit à un sous-groupe normal.

Comme on peut s'en douter, ce n'est pas un hasard si l'on utilise le même mot, « normal », pour certaines extensions de corps et pour certains sous-groupes de groupes : ils se correspondent bien...

Un cas important consiste à adjoindre à K une irrationnelle naturelle θ . Alors $K(\theta)$ est extension normale si, et seulement si, c'est le corps de rupture du polynôme minimum de θ , c'est-à-dire si $K(\theta)$ contient tous les conjugués de θ .

Si $K(\theta)$ contient tous les conjugués de θ , l'adjonction de l'irrationnelle naturelle θ réduit le groupe de Galois à un sous-groupe normal.

De plus, le quotient $G(P|K)/G(P|K(\theta))$ est le groupe de Galois de $K(\theta)$ sur K , c'est-à-dire celui du polynôme minimum de θ .

- L'adjonction d'une irrationnelle naturelle de degré 2 marche toujours, car une extension de degré 2 est toujours normale (ce qui correspond au fait qu'un sous-groupe d'indice 2 est toujours normal).

Ainsi, si Δ est le discriminant de $P \in K[X]$ et si $\sqrt{\Delta}$ n'est pas dans K , alors $G(P|K(\sqrt{\Delta}))$ est un sous-groupe normal de $G(P|K)$, le quotient étant le groupe de Galois de $X^2 - \Delta$ sur K .

- Le groupe de Galois de $X^4 - 2$ sur $\mathbb{Q}$ est d'ordre 8, alors que son groupe de Galois sur $\mathbb{Q}(u)$, où $u = \sqrt[4]{2}$ est la racine quatrième réelle positive de 2, est d'ordre 2.

Si l'on écrit $(u, -u, iu, -iu)$ les racines de $X^4 - 2$, alors $G(X^4 - 2|\mathbb{Q}(u))$ est formé de id et $(3\ 4)$.

Mais la substitution de u par iu est un $\mathbb{Q}(i)$ -automorphisme du corps de rupture $\mathbb{Q}(u, i)$, c'est donc un élément de $G(X^4 - 2|\mathbb{Q})$ qui correspond à la permutation $(1\ 3\ 2\ 4)$.

Le calcul

$$(1\ 3\ 2\ 4)(3\ 4)(1\ 3\ 2\ 4)^{-1} = (1\ 2) \notin G(X^4 - 2|\mathbb{Q}(u))$$

montre que $G(X^4 - 2|\mathbb{Q}(u))$ n'est pas un sous-groupe normal de $G(X^4 - 2|\mathbb{Q})$, ce qui correspond bien au fait que $\mathbb{Q}(u)$ ne contient que 2 des 4 conjugués de u , donc n'est pas extension normale de $\mathbb{Q}$.

D'ailleurs, $\mathbb{Q}(u)$ n'est pas stable par $G(X^4 - 2|\mathbb{Q})$, comme le montre la permutation $(1\ 3\ 2\ 4)$ ci-dessus.

Exercices.

1. Calculer les groupes de Galois, sur $\mathbb{Q}$, de

$$X^3 - 3X^2 + 1, \quad X^3 + X + 1 \quad \text{et} \quad X^4 - 4$$

et chercher à les réduire en adjoignant à $\mathbb{Q}$ des éléments algébriques.

2. Montrer que le groupe de Galois de $X^3 - 12X + 4$ est Σ_3 , que la différence de deux racines est un élément primitif du corps de rupture, son polynôme minimum étant

$$X^6 - 72X^4 + 1\,296X^2 - 6\,480.$$

Si x_1 et x_2 sont deux des racines, montrer que l'adjonction de $(x_1 - x_2)^2 - 24$ réduit le groupe de Galois au sous-groupe formé de l'identité et l'échange de x_1 et x_2 ; calculer le polynôme minimum de $(x_1 - x_2)^2 - 24$.

3. Soit K_2 le corps de rupture de $P_2 \in K[X]$. Montrer que l'adjonction à K des racines de P_2 réduit le groupe de Galois de $P_1 \in K[X]$ à un sous-groupe normal : en d'autres termes

$$G(P_1|K_2) \triangleleft G(P_1|K).$$

De plus, si K_1 est le corps de rupture de P_1 sur K (tout cela dans une même clôture algébrique de K bien sûr), alors $G(P_1|K_2)$ est égal à $G(P_1|K_1 \cap K_2)$.

L'extension $K_1 \cap K_2$ est normale sur K et, si α en est un élément primitif, le groupe de Galois de son polynôme est $G(P_1|K) \cap G(P_1|K_1 \cap K_2)$.

En dé
P₁ à u
quand
réduit

4. Calcul

Vérifie

5. Soit K
vérifie

(On se

Montr

6. Pour l

est (-

On po

et la d

7. Si P es
premi

Que se

ordre 8, alors que
la racine quatrième

de $X^4 - 2$, alors

automorphisme du
t de $G(X^4 - 2|\mathbb{Q})$

$X^4 - 2|\mathbb{Q}(u)$

-groupe normal de
le $\mathbb{Q}(u)$ ne contient
extension normale

$- 2|\mathbb{Q}$), comme le

$p = 4$

ébriques.

que la différence de
polynôme minimum

de $x_1 - x_2 = 24$
et l'échange de x_1

ction à K des racines
-groupe normal : en

ns une même clôture
 $\mathbb{Q}_1[K_1 \cap K_2]$.
nt primitif, le groupe

En déduire que si l'adjonction à K des racines de P_2 réduit le groupe de Galois de P_1 à un sous-groupe d'indice m , il en est de même pour le groupe de Galois de P_2 quand on adjoint à K les racines de P_1 ; de plus, le quotient du groupe par le groupe réduit est le même dans les deux cas. C'est la propriété de « réduction réciproque ».

4. Calculer le discriminant de

$$X^3 + aX^2 + pX + q.$$

Vérifier que, si a est nul, on retrouve $-4p^3 - 27q^2$.

5. Soit $K(\theta)$ une extension normale de K . Quelles sont les extensions L de K qui vérifient

$$G(K(\theta)|K) = G(L(\theta)|L) ?$$

(On se place dans une clôture algébrique de K s'il le faut.)

Montrer que la condition nécessaire et suffisante s'écrit

$$K(\theta) \cap L = K.$$

6. Pour p premier, le discriminant du polynôme cyclotomique

$$\Omega_p = 1 + X + \cdots + X^{p-1}$$

est $(-1)^{\frac{p-1}{2}} p^{p-2}$.

On pourra utiliser l'égalité

$$X^p - 1 = (X - 1) \Omega_p$$

et la dériver.

7. Si P est irréductible sur K et si L est une extension normale de K , tous les facteurs premiers de P dans $L[X]$ ont même degré.

Que se passe-t-il si l'on ne suppose pas L normale sur K ?

La correspondance de Galois

On vient de voir que, si l'on augmente le corps de base, on diminue le groupe de Galois.

Une sorte de réciproque est le problème suivant : si H est un sous-groupe du groupe de Galois de $P \in K[X]$ sur K , H est-il le groupe de Galois de P sur une certaine extension L de K ?

S'il en est ainsi, L est nécessairement le corps des points fixes par H . Cette remarque nous amène à étudier le corps des points fixes par un groupe donné d'automorphismes d'un corps.

Le corps fixe d'un groupe d'automorphismes.

De manière générale, si M est un corps et si G est un groupe fini d'automorphismes de M (donc un sous-groupe fini du groupe $\text{Aut} M$ des automorphismes de M), on notera M_G l'ensemble des points fixes par tous les éléments de G : c'est un sous-corps de M , que l'on appelle le **corps fixe** de G .

- Si M est une extension de degré fini de K et si G est le groupe des K -automorphismes de M , alors le corps fixe de G contient K ; il est égal à K si M est une extension normale de K (voir p. 172), mais sinon il peut contenir strictement K .

Exemple usuel : $u = \sqrt[3]{2}$ (racine cubique réelle de 2),

$$G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \text{id},$$

donc le corps fixe de ce groupe de $\mathbb{Q}$ -automorphismes est tout $\mathbb{Q}(\sqrt[3]{2})$.

- Le groupe de Galois de $(X^2 - 2)(X^2 - 3)$ sur $\mathbb{Q}$ est d'ordre 4, formé des permutations suivantes des racines $\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$:

$$\text{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4).$$

Il y a trois sous-groupes propres autres que l'identité, obtenus en prenant l'identité et l'une des trois autres.

Si l'on prend id et $(1\ 2)$, alors $\sqrt{3}$ est fixe, et le corps des points fixes est $\mathbb{Q}(\sqrt{3})$, sur lequel le groupe de Galois de P est justement $\{\text{id}, (1\ 2)\}$.

Le groupe

Partons
le corps fixe
ce qui signifie
Il est resté
les seuls au

Il suffit p
de Galois d
de l'extensi
Si l'on m
du même c

- le grou
 - le deg
 - l'exter
- polynôme

Tout rev
avoir $(n +$

La démo
de G, g_1 ét
doit montr
Pour cel

Ils sont b
corps M_G .
Méthode
changemen

toute famill

De même si l'on prend id et (3 4) : on trouve $\mathbb{Q}(\sqrt{2})$.

Enfin, voyons le groupe G formé de id et (1 2)(3 4) : son corps fixe est le corps des points fixes de

$$\begin{aligned} \lambda_0 + \lambda_1\sqrt{2} + \lambda_2\sqrt{3} + \lambda_3\sqrt{6} \\ \rightarrow \lambda_0 - \lambda_1\sqrt{2} - \lambda_2\sqrt{3} + \lambda_3\sqrt{6} \end{aligned}$$

c'est donc $\mathbb{Q}(\sqrt{6})$ et le groupe de Galois de P sur $\mathbb{Q}(\sqrt{6})$ est formé de celles des quatre permutations qui laissent fixes $\sqrt{6} = \sqrt{2} \cdot \sqrt{3}$: c'est bien le groupe G .

On retrouve, à l'aide de ces trois sous-groupes, les trois seuls corps strictement intermédiaires entre $\mathbb{Q}$ et $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Le groupe de Galois sur le corps fixe.

Partons d'un corps M , d'un groupe fini G d'automorphismes de M , et soit M_G le corps fixe. Alors tout élément de G est bien sûr un M_G -automorphisme de M , ce qui signifie que G est contenu dans le groupe de Galois de M sur M_G .

Il est remarquable qu'il y ait en fait égalité : les éléments du groupe fini G sont les seuls automorphismes de M laissant fixe M_G .

Il suffit pour cela de prouver que l'ordre de G est supérieur à l'ordre du groupe de Galois de M sur M_G . Mais l'ordre de $G(M|M_G)$ est toujours inférieur au degré de l'extension $M : M_G$.

Si l'on montre que l'ordre de G est supérieur au degré $M : M_G$, on aura prouvé du même coup que

- le groupe G est le groupe de tous les automorphismes de M laissant fixe M_G ;
- le degré de l'extension M sur M_G est égal à l'ordre du groupe de Galois ;
- l'extension M de M_G est normale, donc corps de rupture d'un certain polynôme sur M_G .

Tout revient maintenant à vérifier que, si n est l'ordre de G , il ne peut pas y avoir $(n + 1)$ éléments de M linéairement indépendants sur M_G .

La démonstration est purement technique. On appelle $g_1, \dots, g_n$ les éléments de G , g_1 étant l'identité, on prend $x_1, \dots, x_{n+1}$ éléments distincts dans M et on doit montrer qu'ils sont liés sur M_G .

Pour cela, on considère les $(n + 1)$ vecteurs suivants de M^n :

$$\begin{aligned} (g_1(x_1), \dots, g_n(x_1)) &= V_1, \\ &\dots \\ (g_1(x_{n+1}), \dots, g_n(x_{n+1})) &= V_{n+1}. \end{aligned}$$

Ils sont bien sûr liés sur M et on va montrer qu'ils le sont aussi sur le sous-corps M_G .

Méthode usuelle : on écrit une relation de dépendance *minimale*, soit (par un changement éventuel de numérotation)

$$\lambda_1 V_1 + \dots + \lambda_p V_p = 0$$

toute famille de cardinal $(p - 1)$ étant libre.

de Galois

liminue le groupe de

t un sous-groupe du
Galois de P sur une

s fixes par H . Cette
ar un groupe donné

est un groupe fini
groupe $\text{Aut} M$ des
nts fixes par tous les
e le corps fixe de G .

et si G est le groupe
fixe de G contient K ;
de K (voir p. 172),

elle de 2),

automorphismes est

$X^2 - 3$ sur $\mathbb{Q}$ est
ivantes des racines

4),

l'identité, obtenus en

et le corps des points
ois de P est justement

Les λ_i sont non nuls dans M , tout revient à prouver qu'ils sont en fait dans M_G , c'est-à-dire tous fixes par G .

On écrit donc

$$(1) \quad \lambda_1 g_1(x_1) + \cdots + \lambda_p g_p(x_p) = 0$$

pour tout $i = 1, 2, \dots, n$; on applique un élément g arbitraire de G , ce qui donne

$$g(\lambda_1) g g_1(x_1) + \cdots + g(\lambda_p) g g_p(x_p) = 0.$$

Mais quand i varie de 1 à n , $g g_i$ décrit tout le groupe G , d'où, pour tout i , l'égalité

$$(2) \quad g(\lambda_1) g_1(x_1) + \cdots + g(\lambda_p) g_p(x_p) = 0.$$

On pouvait dès le départ supposer $\lambda_1 = 1$, d'où $g(\lambda_1) = 1$. Dans ces conditions, si, pour $i \neq 1$, $g(\lambda_i)$ est différent de λ_i , on trouve par différence entre (1) et (2) une relation de dépendance entre $(p-1)$ des V_i , ce qui est faux. Donc les λ_j sont tous fixes par G , ils sont dans le sous-corps M_G et les relations de dépendance (1) sont à coefficients dans M_G .

Mais g_1 est l'identité. En prenant $i = 1$, il reste

$$\lambda_1 x_1 + \cdots + \lambda_p x_p = 0$$

avec les λ_i dans M_G et non nuls, d'où la dépendance des x_i sur M_G .

La correspondance de Galois.

Dans tout ce qui précède, on voit se profiler une certaine correspondance entre les corps intermédiaires entre K et une extension M , d'une part, les sous-groupes du groupe de Galois $G(M|K)$, d'autre part.

Plus précisément, soit L un corps intermédiaire

$$K \subset L \subset M.$$

Alors le groupe de Galois de M sur L est un sous-groupe du groupe de Galois de M sur K : c'est le sous-groupe des automorphismes de M laissant fixes non seulement K , mais L tout entier.

Peut-on, inversement, « récupérer » L à partir du groupe de Galois $G(M|L)$?

Oui, si M est extension normale de L , car alors L est le corps fixe de $G(M|L)$. Or M sera normale sur L dès qu'elle le sera sur K : elle est alors engendrée aussi bien sur K que sur L par les racines d'un polynôme sur K .

D'où l'idée de partir d'une extension M normale de K , c'est-à-dire en fait d'un polynôme $P \in K[X]$, dont M sera le corps de rupture, aussi bien sur K que sur les corps intermédiaires.

Dans ces conditions

- au corps intermédiaire L correspond le sous-groupe $G(P|L)$ du groupe $G(P|K)$ et L est le corps fixe du groupe d'automorphismes $G(P|L)$ du corps M (ce groupe étant lui-même sous-groupe du groupe des permutations des racines de P);

LA CORRESPONDANCE

- au sous-groupe G est le groupe

C'est là la correspondance

- à G sous-groupe

- à L corps

- groupe de

- l'indice du

Une remarque.

Le groupe de Galois d'un nombre fini de corps intermédiaires est d'ailleurs vrai, extension de Galois (encore...) le théorème que l'on n'a pas

Extensions normales

Il y a mieux... (voir p. 209) que, restant dans le cas d'un sous-groupe normal. Plus précisément

qui est un homomorphisme

Galois de P sur K

On énoncera

- si L est extension normale de K , le groupe normal d'automorphismes

Cette similitude

l'on démontre le

Galois $G(P|K)$, le

des points fixes j

Question équivalente

On a vu, au

caractérisé par le

Tout revient à

Galois de P sur

minimum de α si

$$\sigma(\alpha) =$$

$$\beta \text{ conj}$$

nt en fait dans M_G .

de G , ce qui donne

our tout i , l'égalité

$i) = 1$. Dans ces
ar différence entre
est faux. Donc les
et les relations de

sur M_G .

respondance entre
t, les sous-groupes

groupe de Galois
laissant fixes non

e Galois $G(M|L)$?

fixe de $G(M|L)$. Or
gendrée aussi bien

à-dire en fait d'un
n sur K que sur les

$G(P|L)$ du groupe
 $G(L)$ du corps M (ce
ations des racines

• au sous-groupe G du groupe $G(P|K)$ correspond le corps fixe M_G par G et G est le groupe de Galois de P sur M_G .

C'est là la **correspondance de Galois** :

- à G sous-groupe de $G(P|K)$ correspond le corps fixe M_G , sous-corps de M ;
- à L corps intermédiaire entre K et M correspond le sous-groupe $G(P|L)$ du groupe de Galois de P sur K ;
- l'indice du sous-groupe est égal au degré du corps fixe.

Une remarque.

Le groupe de Galois d'un polynôme sur le corps K est fini, donc il n'a qu'un nombre fini de sous-groupes, d'où l'on déduit qu'il n'y a qu'un nombre fini de corps intermédiaires entre un corps K et un corps de rupture sur K ; c'est d'ailleurs vrai, non seulement pour les corps de rupture mais pour toute extension de degré fini sur K , il suffit de prendre la clôture normale. D'où (encore...) le théorème de l'élément primitif (voir p. 113), au moins si l'on vérifie que l'on n'a pas fait là un cercle vicieux...

Extensions normales et sous-groupes normaux.

Il y a mieux... Reprenons la correspondance de Galois ci-dessus. On a montré (voir p. 209) que, si l'on augmente le corps K en une extension *normale*, L (tout en restant dans le corps de rupture M de P sur K), le groupe de Galois est réduit à un sous-groupe *normal*.

Plus précisément, on a défini alors l'application « restriction » suivante :

$$\begin{aligned} \sigma &\rightarrow \sigma|_L \\ G(P|K) &\rightarrow G(L|K) \end{aligned}$$

qui est un homomorphisme surjectif de groupes, dont le noyau est le groupe de Galois de P sur le corps intermédiaire L .

On énoncera :

• si L est extension *normale* de K , le groupe de Galois $G(P|L)$ est un sous-groupe *normal* de $G(P|K)$, le quotient étant $G(L|K)$.

Cette similitude de vocabulaire n'est pas due au hasard... Elle sera complète si l'on démontre la réciproque : si H est un sous-groupe *normal* du groupe de Galois $G(P|K)$, le corps intermédiaire qui lui correspond, c'est-à-dire le corps M_H des points fixes par H , est-il extension *normale* de K ?

Question équivalente : M_H est-elle corps de rupture d'un polynôme sur K ?

On a vu, au moins en caractéristique nulle, qu'un corps de rupture est caractérisé par le fait d'être une extension saturée par conjugaison.

Tout revient à montrer que, si H est un sous-groupe *normal* du groupe de Galois de P sur K , si $\alpha \in M$ est fixe par H et si β est une racine du polynôme minimum de α sur K , alors β est aussi fixe par H . On doit vérifier l'implication

$$\left. \begin{aligned} \sigma(\alpha) = \alpha \text{ pour tout } \sigma \in H \\ \beta \text{ conjugué de } \alpha \text{ sur } K \end{aligned} \right\} \Rightarrow \sigma(\beta) = \beta \text{ pour tout } \sigma \in H.$$

Mais on a montré que le K -isomorphisme « substitution de α par β » de $K(\alpha)$ sur $K(\beta)$ se prolonge en un K -automorphisme du corps de rupture commun de P sur $K(\alpha)$ et sur $K(\beta)$ (voir p. 165). On écrit alors $\beta = \varphi(\alpha)$ pour un certain $\varphi \in G(P|K)$, d'où, pour tout $\sigma \in H$, le calcul

$$\sigma(\beta) = \beta \Leftrightarrow \varphi^{-1}\sigma(\beta) = \varphi^{-1}(\beta) \Leftrightarrow \varphi^{-1}\sigma\varphi(\alpha) = \alpha$$

et la dernière égalité est vraie car, comme H est sous-groupe *normal* de $G(P|K)$, l'élément $\varphi^{-1}\sigma\varphi$ est dans H dès que σ y est, donc il laisse fixe α .

On peut alors affirmer :

Dans la correspondance de Galois, les extensions normales du corps de base correspondent aux sous-groupes normaux du groupe de Galois.

L'exemple él

Bien entendu, si tous les sous-groupes du groupe de Galois de $P \in K[X]$ sur K sont normaux (en particulier si ce groupe est abélien), alors tous les corps intermédiaires entre K et le corps de rupture de P sont des extensions normales de K .

Un rappel : l'adjonction d'un élément θ du corps de rupture réduira le groupe de Galois à un sous-groupe normal si, et seulement si, θ engendre sur K le corps de rupture de son polynôme minimum, c'est-à-dire si les conjugués de θ sont des polynômes en θ (c'est la condition $K \triangleleft K(\theta)$).

Au degré 3.

DE GALOIS

var β » de $K(\alpha)$
commun de P
pour un certain

$= \alpha$

mal de $G(P|K)$,
 α .

is normales du
naux du groupe

$P \in K[X]$ sur K
tous les corps
sions normales

duira le groupe
sur K le corps
es de θ sont des

Des exemples

L'exemple élémentaire.

$P = (X^2 - 2)(X^2 - 3)$ sur $\mathbb{Q}$.

Le corps de rupture est $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, le groupe de Galois est $C_2 \times C_2$, formé des quatre permutations suivantes, parmi les vingt-quatre, des racines $(\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3})$:

id, (1 2), (3 4), (1 2)(3 4).

En dehors de l'identité, il y a trois sous-groupes propres, à côté desquels on écrit le corps fixe (corps sur lequel ils sont groupes de Galois de P) et le polynôme dont ce corps est corps de rupture sur $\mathbb{Q}$:

- {id, (1 2)} $\mathbb{Q}(\sqrt{3})$ $X^2 - 3$
- {id, (3 4)} $\mathbb{Q}(\sqrt{2})$ $X^2 - 2$
- {id, (1 2)(3 4)} $\mathbb{Q}(\sqrt{6})$ $X^2 - 6$.

Il suffit, pour déterminer le corps fixe, d'écrire un élément arbitraire de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, soit

$$\lambda_0 + \lambda_1\sqrt{2} + \lambda_2\sqrt{3} + \lambda_3\sqrt{6}$$

puis de chercher quand cet élément est fixe par le sous-groupe.

On retrouve la liste des trois seuls corps strictement intermédiaires entre $\mathbb{Q}$ et $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ et on remarquera que, contrairement aux deux premiers, le troisième corps n'est corps de rupture sur $\mathbb{Q}$ d'aucun diviseur de P dans $\mathbb{Q}[X]$.

Au degré 3.

Prenons maintenant un exemple où le groupe de Galois a des sous-groupes non normaux (en particulier il doit être non abélien).

Le « plus petit » de ces groupes est le groupe symétrique Σ_3 , et il est groupe de Galois de tout polynôme irréductible de degré 3 dont le discriminant n'a pas de racine carrée.

Prenons $P = X^3 - 2$ sur le corps $\mathbb{Q}$. Son groupe de Galois est bien Σ_3 , ce qui signifie que toutes les permutations des trois racines sont bonnes.

En appelant $x = \sqrt[3]{2}$ la racine cubique réelle de 2, écrivons les trois racines

$$(x, jx, j^2x)$$

le corps de rupture étant $\mathbb{Q}(x, j)$, de degré 6 sur $\mathbb{Q}$.

Comme sous-groupes propres de Σ_3 autres que id , on a le groupe alterné A_3 , normal, et les trois sous-groupes formés de l'identité et une transposition, non normaux.

Voyons de plus près :

- $A_3 = \{\text{id}, (1\ 2\ 3), (1\ 3\ 2)\}$: le corps fixe doit être de degré 2 (égal à l'indice de A_3 dans Σ_3) et l'on constate que j , quotient d'une racine et de sa précédente, est fixe par ce groupe. Le corps fixe est donc

$$\mathbb{Q}(j) = \mathbb{Q}(\sqrt{-3})$$

corps de rupture de $1 + X + X^2$ sur $\mathbb{Q}$, dont le groupe de Galois sur $\mathbb{Q}$ est C_2 ; on retrouve bien le quotient de $\Sigma_3 = G(P|\mathbb{Q})$ par $A_3 = G(P|\mathbb{Q}(j))$;

- $\{\text{id}, (1\ 2)\}$: ici, le corps fixe sera de degré 3 sur $\mathbb{Q}$ et il contient manifestement j^2x . C'est donc $\mathbb{Q}(j^2x)$, extension non normale (heureusement...) de $\mathbb{Q}$;

- pour $\{\text{id}, (2\ 3)\}$ et $\{\text{id}, (1\ 3)\}$, on trouvera respectivement $\mathbb{Q}(x)$ et $\mathbb{Q}(jx)$.

C'est là la liste des quatre corps strictement intermédiaires entre $\mathbb{Q}$ et le corps de rupture de $X^3 - 2$.

On pourrait faire le même raisonnement pour tout polynôme irréductible de degré 3 dont le discriminant n'a pas de racine carrée.

Le polynôme $X^4 + 2$.

Un autre exemple classique est celui du groupe D_8 des isométries du carré. Il possède comme éléments les quatre rotations de $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$ et les quatre symétries, S_1 et S_2 par rapport aux médiatrices, σ_1 et σ_2 par rapport aux diagonales. Les sous-groupes sont, outre lui-même et l'identité :

- $\{\text{id}, R_{\frac{\pi}{2}}, R_{\pi}, R_{\frac{3\pi}{2}}\}$, sous-groupe cyclique normal d'ordre 4 ;
- $\{\text{id}, S_1, S_2, R_{\pi}\}$ et $\{\text{id}, \sigma_1, \sigma_2, R_{\pi}\}$, sous-groupes non cycliques normaux d'ordre 4 (isomorphes à $C_2 \times C_2$) ;

Le groupe de Galois est le quotient des trois

de 2, écrivons les

$\mathbb{Q}$.

1, on a le groupe des de l'identité et

être de degré 2 que j , quotient groupe. Le corps

Groupe de Galois $G(P|\mathbb{Q})$ par

$\mathbb{Q}$ et il contient un non normale

ectivement $\mathbb{Q}(x)$

intermédiaires entre

tout polynôme a pas de racine

D_8 des isométries tre rotations de

par rapport aux

nales. Les sous-

al d'ordre 4;

es non cycliques

• $\{\text{id}, R_\pi\}$, sous-groupe normal d'ordre 2;

• $\{\text{id}, S_1\}, \{\text{id}, S_2\}, \{\text{id}, \sigma_1\}, \{\text{id}, \sigma_2\}$, sous-groupes non normaux d'ordre 2.

Il y aura donc, pour un polynôme dont le groupe de Galois est D_8 , huit corps strictement intermédiaires.

On peut prendre comme exemple $P = X^4 + 2$ sur $\mathbb{Q}$, dont le corps de rupture est $\mathbb{Q}(z, i)$, où $z = \sqrt[4]{2}$ désigne la racine quatrième réelle positive de 2 (par exemple...).

Les conjugués de i sont i et $-i$, ceux de z sont $z, -z, iz, -iz$, et les quatre racines sont

$$\left(\frac{1+i}{z}, \frac{1-i}{z}, \frac{-1+i}{z}, \frac{-1-i}{z} \right).$$

Quand i est fixe, on obtient un groupe cyclique d'automorphismes, engendré par $z \rightarrow iz$ ou $z \rightarrow -iz$, qui seront donc $R_{\frac{\pi}{2}}$ et $R_{\frac{3\pi}{2}}$, alors que R_π est $z \rightarrow -z$.

Les quatre symétries sont celles qui transforment i en $-i$, S_1 et S_2 transformant z en z et $-z$, σ_1 et σ_2 le transformant en iz et $-iz$.

Prenons un exemple dans chaque catégorie de sous-groupes :

• *sous-groupe des rotations* : c'est le groupe des $\mathbb{Q}(i)$ -automorphismes, formé des permutations

$$\text{id}, (1\ 4)(2\ 3), (1\ 2\ 4\ 3), (1\ 3\ 4\ 2).$$

Le corps fixe est, bien sûr, $\mathbb{Q}(i)$, corps de rupture de $X^2 + 1$ sur $\mathbb{Q}$, dont le groupe de Galois est d'ordre 2, quotient des groupes de Galois de $X^4 + 2$ sur $\mathbb{Q}$ et sur $\mathbb{Q}(i)$;

• *sous-groupe engendré par deux symétries « perpendiculaires »* : prenons $\{\text{id}, S_1, S_2, R_\pi\}$, c'est-à-dire le groupe

$$\text{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3).$$

Le corps fixe est de degré 2, et z^2 est fixe, donc le corps fixe est égal à $\mathbb{Q}(z^2) = \mathbb{Q}(\sqrt{2})$, corps de rupture de $X^2 - 2$ sur $\mathbb{Q}$.

En prenant σ_1 et σ_2 au lieu de S_1 et S_2 , on trouverait iz^2 fixe, d'où le corps fixe $\mathbb{Q}(iz^2) = \mathbb{Q}(\sqrt{-2})$, corps de rupture de $X^2 + 2$ sur $\mathbb{Q}$;

• *sous-groupe engendré par la rotation d'ordre 2* : le groupe $\{\text{id}, R_\pi\}$ est formé de la permutation identique et de $(1\ 4)(2\ 3)$, son corps fixe est de degré 4 et comprend i et z^2 , c'est

donc $\mathbb{Q}(i, \sqrt{2})$, extension normale de $\mathbb{Q}$ car le sous-groupe est normal dans le groupe de Galois de $X^4 + 2$.

C'est d'ailleurs le corps de rupture de $(X^2 + 1)(X^2 - 2)$, un élément primitif étant $i + \sqrt{2}$: son adjonction réduit donc le groupe de Galois à un sous-groupe normal d'ordre 2 ;

• *sous-groupe engendré par une symétrie* : prenons par exemple le sous-groupe $\{\text{id}, \sigma_1\}$. La permutation des racines correspondant à l'automorphisme σ_1 (qui transforme i en $-i$ et z en iz) est $(1\ 4)$, elle laisse fixes les deux racines $\frac{1-i}{z}$ et $\frac{-1+i}{z}$ de $X^4 + 2$, son corps fixe sera donc $\mathbb{Q}\left(\frac{1-i}{z}\right)$.

Pour $\{\text{id}, \sigma_2\}$, on trouverait $\mathbb{Q}\left(\frac{1+i}{z}\right)$, alors que $\{\text{id}, S_1\}$ et $\{\text{id}, S_2\}$ auront pour corps fixes $\mathbb{Q}(z)$ et $\mathbb{Q}(iz)$, engendrés par des racines quatrièmes de 2, l'une réelle l'autre non réelle. Aucune de ces extensions de $\mathbb{Q}$ n'est normale.

• D'où la liste suivante des corps strictement intermédiaires entre $\mathbb{Q}$ et le corps de rupture de $X^4 + 2$:

- trois extensions quadratiques $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-2})$;
- une extension normale de degré 4, $\mathbb{Q}(i, \sqrt{2})$;
- quatre extensions non normales de degré 4, $\mathbb{Q}(y)$ et $\mathbb{Q}(iy)$ d'une part (en appelant y une racine quatrième donnée de -2), $\mathbb{Q}(z)$ et $\mathbb{Q}(iz)$ de l'autre (en appelant z une racine quatrième donnée de 2).

Le calcul du groupe d'un polynôme irréductible de degré 4.

Les résultats précédents vont nous permettre de reconnaître facilement le groupe de Galois d'un polynôme irréductible de degré 4 sur un corps K .

1° Commençons par des remarques au sujet de l'équation générale de degré 4. Son groupe de Galois est Σ_4 , d'ordre 24, dont les seuls sous-groupes normaux autres que lui et $\{\text{id}\}$ sont A_4 , groupe des douze permutations paires, et le groupe H formé de id , $(1\ 2)(3\ 4)$, $(1\ 3)(2\ 4)$ et $(1\ 4)(2\ 3)$; ce groupe H est isomorphe à $C_2 \times C_2$, on l'appelle parfois le groupe de Klein.

Le corps fixe K_H est une extension normale de degré $\frac{24}{4} = 6$ de K et il contient les éléments

$$y_1 = x_1x_2 + x_3x_4$$

$$y_2 = x_1x_3 + x_2x_4$$

$$y_3 = x_1x_4 + x_2x_3$$

qui sont c
de Galois

qui est de
remarque

(y

appliquée
(car c'est l'
 Σ_3 ou C_2)
l'un des y
l'équation

En con
 $K(y_1, y_2, y_3)$
est égal.

Autrem
est une fo

2° App
seulement

Son gr
liste des sc
normaux

- le gr
- le gr
- le gr
- les g
- longu
- les gr
- cycle

Ceci dit
 $G \cap H$. E
sont don

En d'au

On calcul

Le disc
groupe d
l'homom
du corps

le sous-groupe est 2.

$X^2 + 1)(X^2 - 2)$, un action réduit donc le d'ordre 2;

onons par exemple le cines correspondant i et z en iz est (1 4), $+ i$ de $X^4 + 2$, son

lors que $\{id, S_1\}$ et

, engendrés par des on réelle. Aucune de

nent intermédiaires

$\sqrt{2}$, $\mathbb{Q}(\sqrt{-2})$;

$\sqrt{2}$;

gré 4, $\mathbb{Q}(y)$ et $\mathbb{Q}(iy)$ me donnée de -2 , le quatrième donnée

naître facilement le ir un corps K.

générale de degré 4. s-groupes normaux s paires, et le groupe e H est isomorphe à

6 de K et il contient

qui sont conjugués entre eux (les x_i sont les racines de l'équation). Mais le groupe de Galois de $K(y_1, y_2, y_3)$ est le groupe du polynôme

$$(X - y_1)(X - y_2)(X - y_3)$$

qui est de degré 3 et de discriminant Δ égal à celui de l'équation générale : cette remarque résulte de l'égalité

$$(y_1 - y_2) = x_1(x_2 - x_3) - x_4(x_2 - x_3) = (x_1 - x_4)(x_2 - x_3)$$

appliquée à chaque couple d'indices. Comme $\sqrt{\Delta}$ n'est pas dans le corps de base (car c'est l'équation générale), le groupe de Galois de cette équation de degré 3 est Σ_3 ou C_2 (voir p. 150); c'est C_2 si le polynôme est réductible, ce qui veut dire que l'un des y_i est dans K, et contredit l'indépendance algébrique des racines de l'équation générale.

En conclusion, le groupe de Galois de $K(y_1, y_2, y_3)$ sur K est d'ordre 6, donc $K(y_1, y_2, y_3)$, qui est contenu dans le corps fixe de H et a même degré (égal à 6), lui est égal.

Autrement dit, toute fonction rationnelle des racines x_i , fixe par le groupe H, est une fonction rationnelle des y_i .

2° Appliquons ces résultats à un polynôme de degré 4, que l'on supposera seulement irréductible. Soit

$$P = X^4 - \alpha_1 X^3 + \alpha_2 X^2 - \alpha_3 X + \alpha_4 \in K[X].$$

Son groupe de Galois G est un sous-groupe transitif de Σ_4 . On vérifie que la liste des sous-groupes transitifs de Σ_4 est la suivante (seuls les trois premiers sont normaux et seuls le second et le troisième sont dans A_4) :

- le groupe Σ_4 tout entier, d'ordre 24;
- le groupe alterné A_4 , d'ordre 12;
- le groupe H précédent, d'ordre 4 (non cyclique);
- les groupes cycliques C_4 d'ordre 4, chacun engendré par un cycle de longueur 4;
- les groupes diédraux D_8 d'ordre 8, chacun engendré par le groupe H et un cycle de longueur 4 (isomorphes au groupe des isométries d'un carré).

Ceci dit, l'étude précédente nous incite à réduire le groupe de Galois, de G à $G \cap H$. En effet, le corps fixe correspondant à $G \cap H$ est $K(y_1, y_2, y_3)$ où les y_i sont donnés en fonction des racines x_i de P par les formules antérieures.

En d'autres termes, le corps fixe de $G \cap H$ est le corps de rupture de

$$T = (X - y_1)(X - y_2)(X - y_3).$$

On calcule, à l'aide des fonctions symétriques

$$T = X^3 - \alpha_2 X^2 + (\alpha_1 \alpha_3 - 4\alpha_4)X - \alpha_1^2 \alpha_4 - \alpha_3^2 + 4\alpha_2 \alpha_4.$$

Le discriminant Δ de T est, on l'a vu, le même que celui de P. Quant à son groupe de Galois, c'est le quotient $G' = G/(G \cap H)$: comme toujours, l'homomorphisme « restriction » du groupe de Galois G des K-automorphismes du corps de rupture de P dans le groupe de Galois des K-automorphismes du

corps de rupture de T est surjectif et son noyau est le groupe de Galois de P sur $K(y_1, y_2, y_3)$, donc $G \cap H$ (ceci ne suppose pas d'ailleurs l'irréductibilité de P).

Dans ces conditions, G' , groupe de Galois d'un polynôme de degré 3, est d'ordre 1 ou 2 si T est réductible, d'ordre 3 ou 6 si T est irréductible et, dans chaque cas, tout dépend de $\sqrt{\Delta}$ (voir p. 150).

Or les cinq cas possibles pour G donnent

$$\begin{aligned} G = \Sigma_4 &\Rightarrow G \cap H = H \Rightarrow G' \text{ d'ordre } 6 \Rightarrow G' = \Sigma_3 \\ G = A_4 &\Rightarrow G \cap H = H \Rightarrow G' \text{ d'ordre } 3 \Rightarrow G' = A_3 \\ G = H &\Rightarrow G \cap H = H \Rightarrow G' \text{ d'ordre } 1 \Rightarrow G' = \{\text{id}\} \\ C = C_4 &\Rightarrow G \cap H = C_2 \Rightarrow G' \text{ d'ordre } 2 \Rightarrow G' = C_2 \\ G = D_8 &\Rightarrow G \cap H = H \Rightarrow G' \text{ d'ordre } 2 \Rightarrow G' = C_2. \end{aligned}$$

Ce tableau montre que, à ce stade, la connaissance de G' entraîne celle de G , sauf dans le cas $G' = C_2$ où il faut départager les candidats C_4 et D_8 pour G . On remarque pour cela que $\sqrt{\Delta}$ n'est pas dans le corps de base dans ce cas (voir p. 150), donc son adjonction réduit le groupe de Galois à un sous-groupe d'indice 2, donc d'ordre 2 et 4 respectivement : plus précisément, ce sont $C_4 \cap A_4 = C_2$ et $D_8 \cap A_4 = H$. Le second est transitif et pas le premier, donc, dans le cas $G' = C_2$, le groupe G est C_4 si P est réductible sur $K(\sqrt{\Delta})$, D_8 sinon.

D'où le tableau suivant, qui ramène l'étude du groupe de Galois du polynôme irréductible P de degré 4 à l'étude d'un polynôme T de degré 3, ayant même discriminant Δ :

- $\sqrt{\Delta} \notin K$ et T irréductible $\Leftrightarrow G = \Sigma_4$;
- $\sqrt{\Delta} \in K$ et T irréductible $\Leftrightarrow G = A_4$;
- T totalement factorisable dans K $\Leftrightarrow G = C_2 \times C_2$;
- $\left\{ \begin{array}{l} T \text{ a une seule racine dans } K \\ P \text{ réductible sur } K(\sqrt{\Delta}) \end{array} \right\} \Leftrightarrow G = C_4$;
- $\left\{ \begin{array}{l} T \text{ a une seule racine dans } K \\ P \text{ irréductible sur } K(\sqrt{\Delta}) \end{array} \right\} \Leftrightarrow G = D_8$.

On rappelle que le discriminant de

$$X^3 + a_1X^2 + a_2X + a_3$$

est

$$\Delta = 18a_1a_2a_3 - 4a_1^3a_3 + a_1^2a_2^2 - 4a_2^3 - 27a_3^2.$$

Et si Δ possède une racine carrée dans K , le groupe de Galois ne peut être que A_4 ou H , car aucun des autres n'est dans A_4 ; tout dépendra alors de l'existence ou non d'une racine de T dans K .

- Soit r un rationnel positif. Alors l'irréductibilité de $X^4 + r$ sur $\mathbb{Q}$ équivaut à $\sqrt[4]{4r} \notin \mathbb{Q}$ (voir p. 158).

On calcule

$$T = X^3 - 4rX = X(X^2 - 4r)$$

le Galois de P sur $\mathbb{Q}$ (réductibilité de P).
 le de degré 3, est réductible et, dans

- = Σ_3
- = A_3
- = $\{id\}$
- = C_2
- = C_2 .

entraîne celle de G , et D_8 pour G . On dans ce cas (voir is-groupe d'indice 4) $C_4 \cap A_4 = C_2$ donc, dans le cas D_8 sinon.

Galois du polynôme de degré 3, ayant même

qui possède dans $\mathbb{Q}$ une ou trois racines suivant les cas $\sqrt{r} \notin \mathbb{Q}$ et $\sqrt{r} \in \mathbb{Q}$.

Pour $\sqrt{r} \in \mathbb{Q}$, on trouve

$$G(X^4 + r) = C_2 \times C_2.$$

Mais si $\sqrt{r}$ n'est pas dans $\mathbb{Q}$, on calcule $\Delta = (16r)^2$, et P sera réductible sur $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{r})$ si, et seulement si, on a $\sqrt[4]{4r} \in \mathbb{Q}(\sqrt{r})$, ce qui entraîne

$$\sqrt[4]{4r} = a + b\sqrt{r}$$

avec a et b dans $\mathbb{Q}$, d'où $2\sqrt{r} = a^2 + rb^2 + 2ab\sqrt{r}$, d'où encore

$$\left. \begin{array}{l} a^2 + rb^2 = 0 \\ ab = 1 \end{array} \right\} \text{ et enfin } a^4 + r = 0$$

ce qui est impossible car r est positif.

Bref, pour $\sqrt{r} \notin \mathbb{Q}$, on se trouve dans le cas $G = D_8$.

Ces résultats ont déjà été démontrés (voir p. 160).

• De même, pour un rationnel r positif, l'irréductibilité de $X^4 - r$ sur $\mathbb{Q}$ équivaut à $\sqrt{r} \notin \mathbb{Q}$.

On calcule ici

$$T = X^3 + 4rX = X(X^2 + 4r)$$

qui a toujours une seule racine dans $\mathbb{Q}$, puisque $X^2 + 4r$ n'en a pas. Le discriminant est $\Delta = -(16r)^2$ et le groupe de Galois sera C_4 si $X^4 - r$ est réductible sur $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{-r})$, D_8 sinon.

La première hypothèse s'écrit $\sqrt{r} \in \mathbb{Q}(\sqrt{-r})$, ce qui entraîne $\mathbb{Q}(\sqrt{r}) = \mathbb{Q}(\sqrt{-r})$ pour raisons de degré : c'est impossible, car l'un est contenu dans $\mathbb{R}$ et pas l'autre.

On retrouve bien

$$\sqrt{r} \notin \mathbb{Q} \Rightarrow G(X^4 - r) = D_8.$$

• Retrouvons aussi les résultats concernant un polynôme pair de degré 4, irréductible :

$$P = X^4 + aX^2 + b$$

avec $\sqrt{a^2 - 4b} \notin K$ et $\sqrt{2\sqrt{b} - a} \notin K$.

Le polynôme T se calcule facilement

$$T = X^3 - aX^2 - 4bX + 4ab.$$

Or a est racine évidente et il reste

$$T = (X - a)(X^2 - 4b).$$

Une première conséquence : si $\sqrt{b}$ est dans K , T est totalement factorisable et le groupe de Galois de P est $C_2 \times C_2$ comme on l'a déjà vu.

Supposons maintenant $\sqrt{b} \notin K$. On trouvera le groupe C_4 si P est réductible sur $K(\sqrt{\Delta})$, le groupe D_8 sinon.

On calcule

$$\Delta = (a + 2\sqrt{b})^2(a - 2\sqrt{b})^2(4\sqrt{b})^2$$

$$\text{soit } \Delta = 16(a^2 - 4b)^2b \quad \text{et} \quad K(\sqrt{\Delta}) = K(\sqrt{b}).$$

La réductibilité de P sur $K(\sqrt{\Delta})$ signifie alors

$$\text{soit } \sqrt{a^2 - 4b} \in K(\sqrt{b}), \quad \text{soit } \sqrt{2\sqrt{b} - a} \in K(\sqrt{b}).$$

La première relation traduit l'égalité des extensions quadratiques par $\sqrt{b}$ et par $\sqrt{a^2 - 4b}$ et, d'après un résultat général (d'ailleurs facile à retrouver), cette égalité équivaut à $\sqrt{b(a^2 - 4b)} \in K$.

Quant à la relation $\sqrt{2\sqrt{b} - a} \in K(\sqrt{b})$, on vérifie qu'elle implique $\sqrt{a^2 - 4b} \in K$, ce qui est contradictoire avec l'irréductibilité de P sur K .

On retrouve toute la discussion déjà vue (voir p. 180).

• Prenons un exemple numérique. On va choisir, pour P , le coefficient de X^2 nul, car alors il en sera de même pour T qui s'écrira $X^3 + pX + q$ et le discriminant commun sera

$$\Delta = -4p^3 - 27q^2.$$

Ainsi,

$$P = X^4 + 2X^3 + 2$$

est irréductible sur $\mathbb{Q}$ (on peut le vérifier directement ou par le critère d'Eisenstein), et on calcule

$$T = X^3 - 8X - 8$$

dont le discriminant est $\Delta = -4(-8)^3 - 27(-8)^2 = 8^2 \times 5$, sans racine carrée dans $\mathbb{Q}$.

De plus, T n'a pas de racine rationnelle : si p et q sont des entiers premiers entre eux, l'égalité $T\left(\frac{p}{q}\right) = 0$ donne

$$p^3 - 8pq^2 - 8q^3 = 0$$

Exercices.

1. Étudier

et cherch

Mêmes

2. En utili

montre;
fixe est

3. Si P est
contenu
groupe
intermé

En dédui
élément
dont l'ir
d'une te

Appliqu
($X^2 - 2$

4. Si θ est
sous-gr

engendr

symétric

En dédu
de $K(\theta)$,

ce qui exige $q|p$, donc $q = 1$, et $p|8q^3$, donc $p|8$, et il suffit de montrer que $\pm 1, \pm 2, \pm 4, \pm 8$ ne sont pas racines.

Dès lors, on peut écrire

$$G(X^4 + 2X^3 + 2) = \Sigma_4.$$

• De même, pour $X^4 + X + 1$, irréductible sur $\mathbb{Q}$, on a vu que l'ordre du groupe de Galois est multiple de 3. En fait, des deux candidats Σ_4 et A_4 , ce sera Σ_4 , car on calcule

$$T = X^3 - 4X - 1 \quad \text{et} \quad \Delta = 229$$

qui n'est pas un carré dans $\mathbb{Q}$.

Exercices.

1. Étudier la correspondance de Galois pour les corps de rupture, sur $\mathbb{Q}$, de

$$X^4 - 2, \quad 1 + X + X^2 + X^3 + X^4, \quad X^4 + 9, \quad X^5 - 2$$

et chercher des éléments primitifs et les corps intermédiaires.

Mêmes questions pour $\mathbb{Q}(\sqrt{2}, \sqrt{5})$, pour les corps cyclotomiques d'indice 8, 12.

2. En utilisant la substitution par $X + 1$

$$R(X) \rightarrow R(X + 1)$$

montrer que le groupe d'automorphismes de $K(X)$ sur K est infini, et que le corps fixe est K .

3. Si P est un polynôme sur K et L une extension arbitraire de K (pas forcément contenue dans le corps de rupture), le groupe de Galois de P sur L est un sous-groupe de son groupe de Galois sur K , et l'on montre que son corps fixe, intermédiaire entre K et le corps de rupture K_1 de P sur K , est égal à $K_1 \cap L$.

En déduire que l'adjonction à K d'une irrationnelle accessoire (c'est-à-dire d'un élément hors du corps de rupture de P) réduit le groupe de Galois à un sous-groupe dont l'indice divise *strictement* le degré de l'élément adjoint. Étudier l'adjonction d'une telle irrationnelle accessoire de degré premier.

Appliquer en adjoignant $i + \sqrt{3}$ à $\mathbb{Q}$ pour réduire le groupe de Galois de $(X^2 - 2)(X^2 - 3)$.

4. Si θ est un élément primitif du corps de rupture de $P \in K[X]$ sur K et si H est un sous-groupe du groupe de Galois de P sur K , montrer que le corps fixe de H est engendré sur K par les coefficients de $\prod_{\sigma \in H} (X - \sigma(\theta))$, c'est-à-dire par les fonctions symétriques élémentaires de la suite des $\sigma(\theta)$ quand σ décrit H .

En déduire que si $\alpha \in K(\theta)$ est fixe par H et par aucun autre K -automorphisme de $K(\theta)$, alors α est élément primitif du corps fixe de H sur K .

5. Dans $K(X)$, on appelle σ_1 et σ_2 les substitutions respectives par $\frac{1}{X}$ et $1 - X$.

Montrer que σ_1 et σ_2 engendrent un groupe G d'ordre 6, et que

$$S = \frac{(X^2 - X + 1)^3}{X^2(X - 1)^2}$$

est fixe par G .

Vérifier que $K(X)$ est de degré 6 sur $K(S)$ et que $K(S)$ est le corps fixe de $K(X)$ par G .

Si, au lieu de σ_1 et σ_2 , on prend σ_1 ou σ_2 , des éléments primitifs des corps fixes sont respectivement

$$X + \frac{1}{X} \quad \text{et} \quad X(1 - X).$$

En déduire les degrés.

6. Dans la correspondance de Galois, à des sous-groupes conjugués (c'est-à-dire images l'un de l'autre par conjugaison du groupe) correspondent des corps intermédiaires conjugués (c'est-à-dire images l'un de l'autre par K -automorphismes du corps de rupture du polynôme).

Comparer le groupe de Galois de P sur un corps intermédiaire L et sur la clôture normale de L .

7. Si θ est dans le corps de rupture de P sur K et si $K(\theta)$ est extension normale de K , on a vu que $G(K(\theta)|K)$ est le groupe quotient de $G(P|K)$ par son sous-groupe normal $G(P|K(\theta))$.

Supposons maintenant que $K(\theta)$ ne soit pas forcément extension normale de K et appelons T le polynôme minimum de θ sur K . En considérant encore un homomorphisme « restriction », on montrera que $G(T|K)$ est égal au quotient de $G(P|K)$ par le plus grand sous-groupe normal de $G(P|K)$ contenu dans $G(P|K(\theta))$, ou intersection de ce dernier avec ses conjugués.

8. Dans la correspondance de Galois, si H_1 et H_2 sont les groupes dont les corps fixes sont K_1 et K_2 , alors aux corps K_1K_2 et $K_1 \cap K_2$ correspondent le groupe $H_1 \cap H_2$ et le groupe engendré par H_1 et H_2 .

9. Soit G un sous-groupe de Σ_n . Montrer qu'il existe une extension K du corps des fractions rationnelles à n indéterminées sur $\mathbb{Q}$ telle que le groupe de Galois de l'équation générale de degré n sur ce corps K soit G .

En déduire que tout groupe fini est le groupe de Galois d'un certain polynôme sur un certain corps. Ce que l'on ne sait pas, c'est si l'on peut imposer ce corps de base...

Récapitul

ou racines d
base est $\mathbb{Q}$) :

- le group
- toutes les pu
- ces élér
- conjugués e
- cyclotomiqu
- (nombre d'er
- pour n j

est irréductib

- construi
- polygone rég
- donné à X^n -
- cyclotomique
- un auto
- racine primit
- automorphis
- le group
- multiplicatif
- si n est p

Quelques rac

Pour les p
On écrit d
primitives, et

2	1	[
3	1	[
4	1	-
6	1	
8	1	-

par $\frac{1}{X}$ et $1 - X$.
que

fixe de $K(X)$ par G .
des corps fixes sont

conjugués (c'est-à-dire
sont conjugués des corps
de l'autre par

sur L et sur la clôture

on normale de K , on
sous-groupe normal

on normale de K et
considérant encore un
égal au quotient de
dans $G(P|K(\theta))$,

dont les corps fixes
sont conjugués le groupe

on K du corps des
groupe de Galois de

certain polynôme sur
ce corps de base...

Quelques racines de l'unité

Récapitulons quelques propriétés du groupe G_n des racines n -ièmes de l'unité, ou racines du polynôme $X^n - 1$, formant la suite $(e^{\frac{2ik\pi}{n}})_{k=0,1,\dots,n-1}$ (le corps de base est $\mathbb{Q}$) :

- le groupe G_n est cyclique d'ordre n , engendré par $\omega_n = e^{\frac{2i\pi}{n}}$ et aussi par toutes les puissances ω_n^m où m est premier avec n ;
- ces éléments ω_n^m , appelés racines primitives n -ièmes de l'unité, sont conjugués entre eux; leur polynôme minimum commun, appelé polynôme cyclotomique d'indice n et noté Φ_n , est un diviseur de $X^n - 1$, de degré $\varphi(n)$ (nombre d'entiers inférieurs à n premiers avec n);
- pour n premier, $\varphi(n)$ est égal à $(n - 1)$, et le polynôme

$$\frac{X^n - 1}{X - 1} = 1 + X + \dots + X^{n-1}$$

est irréductible, donc c'est le polynôme Φ_n ;

- construire une racine primitive n -ième de l'unité signifie construire un polygone régulier de n côtés, d'où le nom d'équation de la division du cercle donné à $X^n - 1 = 0$; de même, le corps de rupture de $X^n - 1$ est appelé corps cyclotomique d'indice n (cyclotomique = divisant le cercle);

- un automorphisme du corps cyclotomique est donné par l'image d'une racine primitive ω_n , laquelle est une racine primitive ω_n^m , et la composition des automorphismes correspond au produit modulo n des exposants;

- le groupe de Galois du corps cyclotomique d'indice n est le groupe multiplicatif $(\mathbb{Z}/n)^*$ des entiers modulo n premiers avec n , son ordre est $\varphi(n)$;

- si n est premier, ce groupe est $(\mathbb{Z}/n)^*$, il est cyclique et isomorphe à C_{n-1} .

Quelques racines simples de l'unité.

Pour les premières valeurs de n , il est facile de calculer les racines de l'unité. On écrit dans ce qui suit la valeur de n , les racines de l'unité en encadrant les primitives, et le polynôme cyclotomique.

2	1	$\boxed{-1}$							$1 + X$
3	1	$\boxed{j}$	$\boxed{j^2}$						$1 + X + X^2$
4	1	-1	$\boxed{i}$	$\boxed{-i}$					$1 + X^2$
6	1	j	j^2	-1	$\boxed{-j}$	$\boxed{-j^2}$			$1 - X + X^2$
8	1	-1	i	$-i$	$\boxed{\frac{1+i}{\sqrt{2}}}$	$\boxed{\frac{1-i}{\sqrt{2}}}$	$\boxed{\frac{-1+i}{\sqrt{2}}}$	$\boxed{\frac{-1-i}{\sqrt{2}}}$	$1 + X^4$

Les premiers « trous » concernent les racines cinquième et septième. C'est leur calcul que l'on va exposer maintenant.

On notera aussi que la constructibilité à la règle et au compas du polygone de n cotés exige que $\varphi(n)$, degré du corps cyclotomique, soit une puissance de 2 (on verra plus loin que c'est suffisant).

Prenons p premier. Alors $\varphi(p)$ est égal à $p - 1$, et p doit être somme de 1 et d'une puissance de 2. Les plus petites valeurs de p sont 5 et 17, c'est pourquoi on étudiera aussi les racines primitives dix-septièmes de l'unité.

On montrera plus tard pourquoi toutes ces racines p -ièmes s'expriment à l'aide de radicaux d'indices premiers strictement inférieurs à p (voir p. 251).

Les racines cinquièmes de l'unité.

Les quatre racines cinquièmes de l'unité autres que 1 sont primitives, racines du polynôme cyclotomique

$$\Phi_5 = 1 + X + X^2 + X^3 + X^4.$$

Soit ω l'une d'elles (par exemple $e^{\frac{2i\pi}{5}}$). Les générateurs du groupe multiplicatif $(\mathbb{Z}/5)\backslash 0$ sont 2 ou 3. Ainsi la suite des puissances de 2 est (2, 4, 3, 1), donc le groupe de Galois G du polynôme Φ_5 est cyclique, engendré par le cycle

$$\sigma : (\omega, \omega^2, \omega^4, \omega^3).$$

Le calcul des racines de Φ_5 peut se faire à l'aide de la méthode générale exposée pour les polynômes de degré 4. On va plutôt utiliser la réduction du groupe de Galois et on va arriver à une expression ne faisant intervenir que des racines carrées (et aucune cubique).

On passe de C_4 à id à l'aide du groupe intermédiaire C_2 qui est le sous-groupe de G engendré par σ^2 . Le corps intermédiaire entre $\mathbb{Q}$ et $\mathbb{Q}(\omega)$ est une extension quadratique de $\mathbb{Q}$, engendrée par tout élément fixe par σ^2 et pas par σ . Un candidat simple est

$$\alpha = \omega + \sigma^2(\omega)$$

c'est-à-dire

$$\alpha = \omega + \omega^4 = 2 \cos \frac{2\pi}{5}.$$

Son conjugué, autre que lui-même, est

$$\sigma(\alpha) = \omega^2 + \omega^3 = 2 \cos \frac{4\pi}{5}$$

et on calcule $\alpha + \sigma(\alpha) = -1$ et $\alpha\sigma(\alpha) = -1$, ce qui donne α et $\sigma(\alpha)$ comme racines de $X^2 + X - 1$.

Un pre

Un sec

et ω doit

En effe
permutati
conjugués

Dès lor
être dans

Des deu

on déduit

C'est là
c'est $e^{\frac{2i\pi}{5}}$.

avec ε_1 et
possibles

Si l'on r

Ce dern
par racine

ième. C'est leur

polygone de n
issance de 2 (on

somme de 1 et
st pourquoi on

priment à l'aide
n. 251).

mitives, racines

pe multiplicatif
donc le groupe
le

générale exposée
on du groupe de
que des racines

le sous-groupe
st une extension
pas par σ . Un

et $\sigma(\alpha)$ comme

Un premier résultat :

$$\cos \frac{2\pi}{5} = \frac{-1 + \sqrt{5}}{4}.$$

Un second résultat : le corps fixe de σ^2 est $\mathbb{Q}(\sqrt{5})$, d'où la chaîne

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\omega)$$

et ω doit être de degré 2 sur $\mathbb{Q}(\sqrt{5})$.

En effet, sur $\mathbb{Q}(\sqrt{5})$, ω^2 n'est plus conjugué de ω , σ n'est plus une bonne permutation, le groupe de Galois sur $\mathbb{Q}(\sqrt{5})$ est réduit à $\{\text{id}, \sigma^2\}$, donc les conjugués de ω sont ω et $\sigma^2(\omega) = \omega^4$.

Dès lors, l'élément $\beta = \omega - \omega^4$ a pour conjugués β et $-\beta$, donc son carré doit être dans $\mathbb{Q}(\sqrt{5})$. On calcule en effet

$$\begin{aligned} \beta^2 &= (\omega - \omega^4)^2 = \omega^2 + \omega^3 - 2 = \sigma(\alpha) - 2 \\ &= \frac{-1 - \sqrt{5}}{2} - 2 = \frac{-5 - \sqrt{5}}{2}. \end{aligned}$$

Des deux égalités

$$\begin{cases} \omega + \omega^4 = \alpha \\ \omega - \omega^4 = \beta \end{cases}$$

on déduit $2\omega = \alpha + \beta$, d'où

$$\omega = \frac{-1 + \sqrt{5}}{4} + \frac{i}{2} \sqrt{\frac{5 + \sqrt{5}}{2}}.$$

C'est là une racine cinquième primitive de l'unité, on vérifie d'ailleurs que c'est $e^{\frac{2i\pi}{5}}$. Pour avoir les quatre, on écrit

$$\frac{-1 + \varepsilon_1 \sqrt{5}}{4} + \frac{i}{2} \varepsilon_2 \sqrt{\frac{5 + \varepsilon_1 \sqrt{5}}{2}}$$

avec ε_1 et ε_2 valant $+1$ ou -1 : le choix de ε_1 correspond aux deux valeurs possibles de α , celui de ε_2 aux valeurs de β .

Si l'on récapitule, la correspondance de Galois s'écrit

$$\{\text{id}, \sigma, \sigma^2, \sigma^3\} \supset \{\text{id}, \sigma^2\} \supset \{\text{id}\}$$

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}\left(\sqrt{\frac{-5 - \sqrt{5}}{2}}\right).$$

Ce dernier corps est le corps cyclotomique d'indice 5, c'est une extension de $\mathbb{Q}$ par racines carrées successives.

Le pentagone régulier est constructible à la règle et au compas.

Les racines septièmes de l'unité.

L'équation de la division du cercle est maintenant

$$X^7 - 1 \in \mathbb{Q}[X]$$

le polynôme cyclotomique s'écrivant

$$\Phi_7 = 1 + X + X^2 + X^3 + X^4 + X^5 + X^6.$$

On appellera encore ω une de ses racines, par exemple $e^{\frac{2i\pi}{7}}$. Pour avoir un générateur du groupe de Galois, ou groupe multiplicatif des entiers modulo 7 premiers avec 7, on écrit les suites de puissances des éléments : pour 2, on trouve (2, 4, 1), sous-groupe propre, alors que pour 3 il vient (3, 2, 6, 4, 5, 1), ce qui montre que 3 est un générateur.

Le groupe de Galois est donc engendré par le cycle qui transforme ω en ω^3 , c'est-à-dire

$$\sigma : (\omega, \omega^3, \omega^2, \omega^6, \omega^4, \omega^5),$$

on va le réduire suivant la chaîne $C_6 \supset C_3 \supset \text{id}$.

Le sous-groupe cyclique d'ordre 3 est engendré par σ^2 , son corps fixe sera une extension quadratique de $\mathbb{Q}$ (car l'indice du sous-groupe est 2) engendrée par un élément fixe par σ^2 et pas par σ .

On va prendre

$$\alpha = \omega + \sigma^2(\omega) + \sigma^4(\omega)$$

soit

$$\alpha = \omega + \omega^2 + \omega^4.$$

Comme conjugué de α on trouve

$$\sigma(\alpha) = \omega^3 + \omega^6 + \omega^5 = -1 - \alpha$$

et on calcule directement le produit $\alpha \cdot \sigma(\alpha) = 2$ (en utilisant le fait que la somme des racines primitives est -1). Donc α et $\sigma(\alpha)$ sont les racines de

$$X^2 + X + 2 \in \mathbb{Q}[X]$$

de discriminant -7 , ce qui montre que le corps fixe du sous-groupe $\{\text{id}, \sigma^2, \sigma^4\}$ est $\mathbb{Q}(\sqrt{-7})$.

$$\text{On prendra par exemple } \alpha = \frac{-1 + i\sqrt{7}}{2}.$$

Le groupe de Galois du corps cyclotomique sur $\mathbb{Q}(\sqrt{-7})$ doit être justement $\{\text{id}, \sigma^2, \sigma^4\}$ et ω est de degré 3 sur $\mathbb{Q}(\sqrt{-7})$, ses conjugués étant $\omega, \omega^2, \omega^4$.

D'après l'étude des polynômes de degré 3, il est intéressant de considérer l'élément $\beta = \omega + j\omega^2 + j^2\omega^4$, car ses conjugués sont $\beta, j\beta, j^2\beta$ (on aura au préalable adjoint j , donc $\sqrt{-3}$, au corps de base), ce qui montre que β^3 doit être dans $\mathbb{Q}(j, \sqrt{-7})$.

En effet, c
 β^3

Comme σ

Premier ré

$$\mathbb{Q}(\sqrt{-3}, \sqrt{-7})$$

Second ré:
extractions c
dernière emp
côtés.

On peut f
parallèlement

Le calcul c
remarquer q
En ajouter

on trouve

d'où l'express

où β est une
cubique de 7

En effet, on calcule

$$\begin{aligned}\beta^3 &= 6 + (1 + 3j^2)(\omega^3 + \omega^5 + \omega^6) + 3j(\omega + \omega^2 + \omega^4) \\ &= 6 + \sigma(\alpha) + 3(j\alpha + j^2\sigma(\alpha)) \\ &= 6 + \sigma(\alpha) + 6 \operatorname{Re} j\alpha.\end{aligned}$$

Comme $\sigma(\alpha)$ vaut $\frac{-1 - i\sqrt{7}}{2}$ et $j\alpha$ a pour partie réelle $\frac{1 - \sqrt{21}}{4}$, il reste

$$\beta^3 = 7 - \frac{3}{2}\sqrt{21} - \frac{i}{2}\sqrt{7}.$$

Premier résultat: le corps cyclotomique d'indice 7 est contenu dans l'extension

$$\begin{aligned}\mathbb{Q}\left(\sqrt{-3}, \sqrt{-7}, \sqrt[3]{7 - \frac{3}{2}\sqrt{21} - \frac{1}{2}\sqrt{-7}}\right) \\ = \mathbb{Q}\left(\sqrt{-3}, \sqrt[3]{7 - \frac{3}{2}\sqrt{21} - \frac{1}{2}\sqrt{-7}}\right).\end{aligned}$$

Second résultat : les racines septièmes de l'unité s'écrivent à l'aide de deux extractions de racines carrées et d'une extraction de racine cubique, cette dernière empêchant la construction à la règle et au compas du polynôme de sept côtés.

On peut faire le calcul complet de ces racines. Pour ce faire, on pose, parallèlement à β :

$$\gamma = \omega + j^2\omega^2 + j\omega^4.$$

Le calcul de γ^3 peut se faire directement comme β^3 , mais il est plus simple de remarquer que $\beta\gamma$ est égal à $\alpha - \sigma(\alpha)$ (calcul facile), donc à $i\sqrt{7}$.

En ajoutant les trois égalités

$$\omega + \omega^2 + \omega^4 = \alpha$$

$$\omega + j\omega^2 + j^2\omega^4 = \beta$$

$$\omega + j^2\omega^2 + j\omega^4 = \frac{i\sqrt{7}}{\beta}$$

on trouve
$$3\omega = \alpha + \beta + \frac{i\sqrt{7}}{\beta}$$

d'où l'expression (bien compliquée...) d'une racine primitive septième de l'unité :

$$\omega = \frac{1}{3}\left(\frac{-1 + i\sqrt{7}}{2} + \beta + \frac{i\sqrt{7}}{\beta}\right)$$

où β est une racine cubique de $7 - \frac{3}{2}\sqrt{21} - \frac{i}{2}\sqrt{7}$ (et $\frac{i\sqrt{7}}{\beta}$ est une racine cubique de $7 + \frac{3}{2}\sqrt{21} - \frac{i}{2}\sqrt{7}$).

A partir de ω , les six racines primitives s'obtiennent en donnant à β les trois valeurs possibles, puis en partant de l'expression obtenue en remplaçant, dans l'expression de ω ,

$$\alpha = \frac{-1 + i\sqrt{7}}{2} \quad \text{par} \quad \frac{-1 - i\sqrt{7}}{2} \quad \text{et} \quad \beta \text{ par} \quad 7 + \frac{3}{2}\sqrt{21} + \frac{i}{2}\sqrt{7}.$$

Les racines dix-septièmes de l'unité.

Comme on l'a signalé, le cas des racines dix-septièmes de l'unité est particulièrement intéressant car le degré du corps cyclotomique est 16, c'est-à-dire puissance de 2. On va montrer que ces racines s'expriment à l'aide d'extractions de racines carrées seulement, ce qui entraîne la constructibilité à la règle et au compas du polygone de 17 côtés. La résolution de ce problème géométrique a été l'œuvre de Gauss, bien avant Galois; et Gauss considérait ce résultat comme l'un de ses travaux les plus remarquables.

Les racines dix-septièmes de l'unité autres que 1 sont toutes primitives, leur polynôme minimum commun est

$$\Phi_{17} = 1 + X + X^2 + \cdots + X^{16}.$$

On posera par exemple

$$\omega = e^{\frac{2i\pi}{17}}.$$

Ici encore, il nous faut trouver un générateur du groupe cyclique multiplicatif $(\mathbb{Z}/17)\backslash 0$.

La suite des puissances de 2 est $\{2, 4, 8, 16, 15, 13, 9, 1\}$, donc 2 n'est pas générateur. Par contre, pour 3, on calcule la suite

$$\{3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1\}$$

qui montre que 3 engendre le groupe. Dans ces conditions, on prendra pour générateur du groupe de Galois G de notre corps cyclotomique l'automorphisme σ défini par

$$\sigma: \omega \rightarrow \omega^3.$$

En appelant $[\sigma^i]$ le sous-groupe engendré par σ^i , on écrit la chaîne décroissante de groupes

$$G = [\sigma] \supset [\sigma^2] \supset [\sigma^4] \supset [\sigma^8] \supset \text{id}.$$

La correspondance de Galois doit nous donner la suite croissante des corps fixes, chacun extension quadratique du précédent :

$$\mathbb{Q} \subset K_1 \subset K_2 \subset K_3 \subset K.$$

On va les calculer explicitement.

QUELQUES

• K_1 est en

Un bon can
On posera do

c'est-à-dire

D'ailleurs, s

en groupant c

Notre éléme
sur $\mathbb{Q}$. Il est c

x_2

qui est aussi é

La somme c

On calcule c

et le corps int
Le discriminant

$$K_1 = \mathbb{Q}(\sqrt{17}).$$

• On passe
comme éléme

Sur K_1 , $y_1 \in$

Donc K_2 es

dont le discriminant

$$K_2 = K_1(\sqrt{17}).$$

donnant à β les trois
en remplaçant, dans

$$+ \frac{3}{2}\sqrt{21} + \frac{i}{2}\sqrt{7}.$$

tièmes de l'unité est
omique est 16, c'est-à-
s'expriment à l'aide
la constructibilité à la
tion de ce problème
Gauss considérait ce
s.

toutes primitives, leur

cyclique multiplicatif

, 1}, donc 2 n'est pas

2, 6, 1}

ons, on prendra pour
ique l'automorphisme

la chaîne décroissante

id.

croissante des corps

• K_1 est engendré sur $\mathbb{Q}$ par tout élément fixe par σ^2 et pas par σ .

Un bon candidat sera la somme des images de ω par les puissances paires de σ .
On posera donc

$$x_1 = \omega + \sigma^2(\omega) + \sigma^4(\omega) + \cdots + \sigma^{14}(\omega)$$

c'est-à-dire

$$x_1 = \sum_{i=0}^7 \omega^{3^{2i}}.$$

D'ailleurs, si l'on pose $\theta = \frac{2\pi}{17}$, on calcule

$$x_1 = 2(\cos \theta + \cos 8\theta + \cos 4\theta + \cos 2\theta)$$

en groupant chaque $\sigma^{2^i}(\omega)$ avec son inverse (qui est son conjugué complexe).

Notre élément x_1 , fixe par σ^2 et pas par σ , est racine d'une équation de degré 2 sur $\mathbb{Q}$. Il est conjugué de

$$x_2 = \sigma(x_1) = \sigma(\omega) + \sigma^3(\omega) + \sigma^5(\omega) + \cdots + \sigma^{15}(\omega)$$

qui est aussi égal à

$$x_2 = 2(\cos 3\theta + \cos 7\theta + \cos 5\theta + \cos 6\theta).$$

La somme des racines primitives vaut -1 , ce qui donne $x_1 + x_2 = -1$.

On calcule directement $x_1 x_2 = -4$, donc x_1 et x_2 sont les racines de

$$X^2 + X - 4$$

et le corps intermédiaire K_1 est le corps de rupture de ce polynôme sur $\mathbb{Q}$.
Le discriminant vaut 17 et on écrit alors

$$K_1 = \mathbb{Q}(\sqrt{17}), \quad x_1 = \frac{-1 + \sqrt{17}}{2} \quad \text{et} \quad x_2 = \frac{-1 - \sqrt{17}}{2}.$$

• On passe à K_2 , corps fixe de σ^4 et extension quadratique de K_1 . On prend
comme élément primitif de K_2 sur K_1 :

$$\begin{aligned} y_1 &= \omega + \sigma^4(\omega) + \sigma^8(\omega) + \sigma^{12}(\omega) \\ &= 2(\cos \theta + \cos 4\theta). \end{aligned}$$

Sur K_1 , y_1 est conjugué de $y_2 = \sigma^2(y_1)$ et on calcule

$$y_1 + y_2 = x_1 \quad \text{et} \quad y_1 y_2 = -1.$$

Donc K_2 est corps de rupture, sur K_1 , du polynôme

$$X^2 - x_1 X - 1$$

dont le discriminant est $x_1^2 + 4 = 8 - x_1$. On écrira

$$K_2 = K_1(\sqrt{8 - x_1}), \quad y_1 = \frac{x_1 + \sqrt{8 - x_1}}{2} \quad \text{et} \quad y_2 = \frac{x_1 - \sqrt{8 - x_1}}{2}.$$

D'ailleurs, $8 - x_1$ est égal à

$$8 - x_1 = 8 - \frac{-1 + \sqrt{17}}{2} = \frac{17 - \sqrt{17}}{2}$$

ce qui permet d'écrire

$$K_2 = \mathbb{Q}(\sqrt{2(17 - \sqrt{17})})$$

extension de degré 4.

- Au tour de K_3 , corps fixe de σ^8 , engendré sur K_2 par

$$\begin{aligned} z_1 &= \omega + \sigma^8(\omega) \\ &= 2 \cos \theta. \end{aligned}$$

Même processus : conjugué $z_2 = \sigma^4(z_1) = 2 \cos 4\theta$, calculs de

$$z_1 + z_2 = y_1, \quad z_1 z_2 = 2(\cos 5\theta + \cos 3\theta).$$

Le dernier élément est construit à partir de x_2 comme y_1 l'est à partir de x_1 , ce qui donne

$$z_1 z_2 = \frac{x_2 + \sqrt{8 - x_2}}{2} = -\frac{1 + \sqrt{17}}{4} + \frac{1}{2} \sqrt{\frac{17 + \sqrt{17}}{2}}.$$

Appelons α cet élément, qui est dans K_2 . Dès lors K_3 est le corps de rupture, sur K_2 , du polynôme

$$X^2 - y_1 X + \alpha$$

et $z_1 = 2 \cos \frac{2\pi}{17}$ est une racine de ce polynôme.

On pourra écrire

$$K_3 = K_2(\sqrt{y_1^2 - 4\alpha}) = K_2(\sqrt{x_1 y_1 + 1 - 4\alpha})$$

et même calculer explicitement $\cos \frac{2\pi}{17}$ (un peu long...).

- Bien entendu, $\omega = e^{\frac{2\pi i}{17}}$ est de degré 2 sur ce corps K_3 , conjugué sur K_3 de $\sigma^8(\omega)$ qui n'est autre que $e^{-\frac{2\pi i}{17}}$.

Leur somme vaut $z_1 = 2 \cos \frac{2\pi}{17}$ et leur produit vaut 1, ce qui donne le corps engendré sur K_3 par $\sqrt{z_1^2 - 4}$: c'est là notre corps cyclotomique.

Comme on le voit, seules interviennent des racines carrées.

Il est te
résolubles
ses racine
« formule.

En tern
chaîne fini
telle que l
radical ré
Galois de
certaines]

On sup
le corps
contient C

Des exem

Le groupe de Galois d'une équation résoluble

s de

0).

à partir de x_1 , ce qui

$$\frac{-1 \pm \sqrt{17}}{2}$$

corps de rupture, sur

4α)

conjugué sur K_3 de

qui donne le corps

omique.

es.

Il est temps de revenir à l'un de nos problèmes initiaux, celui des équations résolubles. On a dit que l'équation $P(X) = 0$ est résoluble sur le corps K quand ses racines s'expriment algébriquement à partir de K , c'est-à-dire à l'aide de « formules » où n'interviennent que des éléments de K et des radicaux.

En termes plus précis, ceci signifie qu'à partir de K on peut construire une chaîne finie croissante de corps, chacun extension du précédent par un radical, et telle que le dernier contienne toutes les racines de P . Or, chaque adjonction de radical réduit le groupe de Galois d'une certaine manière, donc le groupe de Galois de P sur K aura une chaîne décroissante de sous-groupes possédant certaines propriétés. C'est ce que l'on va examiner.

On supposera, s'il le faut, que l'on est en caractéristique nulle, c'est-à-dire que le corps K (qui sera souvent le corps engendré par les coefficients de P) contient $\mathbb{Q}$.

Des exemples.

- Le corps de rupture de $X^4 - 2$ sur $\mathbb{Q}$ est $\mathbb{Q}(\sqrt[4]{2}, i)$, en appelant $\sqrt[4]{2}$ la racine quatrième réelle positive de 2, par exemple. D'où la chaîne de corps

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2})(i)$$

les groupes de Galois correspondants étant

$$G(P|\mathbb{Q}) = D_8 \text{ (groupe des isométries du carré)}$$

$$G(P|\mathbb{Q}(\sqrt[4]{2})) = C_2$$

$$G(P|\mathbb{Q}(\sqrt[4]{2}, i)) = \text{id.}$$

La chaîne décroissante des groupes est

$$D_8 \supset C_2 \supset \text{id.}$$

On aurait pu aussi prendre pour chaîne de corps

$$\mathbb{Q} \subset \mathbb{Q}(i) \subset \mathbb{Q}(i)(\sqrt[4]{2}).$$

Le groupe de Galois de $X^4 - 2$ sur $\mathbb{Q}(i)$ est cyclique d'ordre 4, engendré par la permutation (1 3 2 4) si l'on écrit les racines

$$(\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2})$$

d'où la chaîne de groupes

$$D_8 \supset C_4 \supset \text{id}.$$

Mais on peut aussi « affiner » la chaîne de corps en adjoignant d'abord $\sqrt{2}$, puis sa racine carrée $\sqrt[4]{2}$. A la chaîne

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2})(i)$$

correspond la chaîne de groupes

$$D_8 \supset C_2 \times C_2 \supset C_2 \supset \text{id}$$

car le groupe de Galois de $X^4 - 2$ sur $\mathbb{Q}(\sqrt{2})$ est $C_2 \times C_2$.

• Pour l'équation générale $X^3 + pX + q = 0$, où p et q sont des indéterminées, on part du corps $K = \mathbb{Q}(p, q)$, et l'on adjoit successivement une racine carrée de -3 , une racine carrée de $\Delta = -4p^3 - 27q^2$, et une racine cubique de

$$u = \frac{-27q + 3\sqrt{-3}\sqrt{\Delta}}{2}.$$

Les racines de $X^3 + pX + q$ sont dans le dernier corps de la chaîne

$$K \subset K(\sqrt{-3}) \subset K(\sqrt{-3})(\sqrt{\Delta}) \subset K(\sqrt{-3})(\sqrt{\Delta})(\sqrt[3]{u}).$$

La chaîne des groupes de Galois est alors

$$\Sigma_3 \supset \Sigma_3 \supset A_3 \supset \text{id}.$$

Premières remarques.

Partons de l'équation $P(X) = 0$ résoluble sur K . Il existe alors une chaîne

$$K \subset K_1 \subset \dots \subset K_{n-1} \subset K_n$$

où

• tout corps est extension du précédent par un radical, c'est-à-dire que l'on peut écrire

$$K_i = K_{i-1}(b_i)$$

avec $b_i^{n_i} \in K_{i-1}$ pour certains exposants n_i ;

• le corps K_n contient toutes les racines de P .

On remarque sur K , mais corps de ru

En fait, on par sa clôture on « allonge

En effet, le produit

en écrivant à radicaux suc

et b_i' , image

car les con invariant.

Quitte à a corps de ru

Ceci dit, extension n contiendra C'est pou

Un cas spéc

Supposon c'est-à-dire l

Alors K_i son groupe d'ordre n_i ; il est de la for des K_{i-1} -au

D'autre p sous-groupe L'homomor

qui est bien c corps de ru

rps

clique d'ordre 4,
écrit les racines

ps en adjoignant
laîne

(i)

est $C_2 \times C_2$.

), où p et q sont
), et l'on adjoit
racine carrée de

nier corps de la

$(-3)(\sqrt{\Delta})(\sqrt[3]{u})$.

ors une chaîne

t-à-dire que l'on

On remarquera qu'il n'est nullement exigé que K_n soit le corps de rupture de P sur K , mais seulement qu'il le contienne. Il n'est pas même exigé que K_n soit un corps de rupture (c'est-à-dire une extension normale).

En fait, on peut supposer que K_n est un corps de rupture, quitte à le remplacer par sa clôture normale qui est encore une extension par radicaux successifs de K : on « allonge » donc la chaîne.

En effet, K_n est égal à $K(b_1, \dots, b_n)$ et sa clôture normale, ou corps de rupture du produit des polynômes minima des b_i sur K , est

$$K(b_1, b'_1, \dots, b_2, b'_2, \dots, b_n, b'_n, \dots)$$

en écrivant à côté de chaque b_i ses conjugués sur K . C'est bien une extension par radicaux successifs : ainsi b_2 vérifie

$$b_2^{n_2} \in K(b_1), \quad \text{d'où} \quad b_2^{n_2} \in K(b_1, b'_1, \dots)$$

et b'_2 , image de b_2 par un K -automorphisme, vérifie aussi

$$b_2'^{n_2} \in K(b_1, b'_1, \dots)$$

car les conjugués de b_1 sont seulement permutés, donc $K(b_1, b'_1, \dots)$ est invariant.

Quitte à allonger la chaîne, on aura donc un polynôme $T \in K[X]$ dont K_n est corps de rupture sur K : c'est le produit des polynômes minima des b_i sur K .

Ceci dit, K_i est engendré sur K_{i-1} par un radical n_i -ième, ce sera donc une extension normale, corps de rupture de $X^{n_i} - b_i^{n_i} \in K_{i-1}[X]$, dès que K_{i-1} contiendra les racines n_i -ièmes de l'unité.

C'est pourquoi on commencera par un cas particulier.

Un cas spécialement simple.

Supposons dès le départ que K contient les racines de l'unité nécessaires, c'est-à-dire les n_i -ièmes pour tout i .

Alors K_i est corps de rupture sur K_{i-1} d'une équation binôme de degré n_i , son groupe de Galois sur K_{i-1} est donc un sous-groupe du groupe cyclique d'ordre n_i ; il est, par suite, cyclique aussi et *a fortiori* abélien. En effet l'image de b_i est de la forme $\omega^t b_i$, où ω est racine primitive n_i -ième de l'unité et la composition des K_{i-1} -automorphismes correspond à l'addition modulo n_i des exposants t .

D'autre part, l'adjonction à K_{i-1} du radical b_i réduit le groupe de Galois à un sous-groupe normal car l'extension contient alors tous les conjugués de b_i . L'homomorphisme « restriction »

$$\begin{aligned} G(K_n | K_{i-1}) &\rightarrow G(K_i | K_{i-1}) \\ \sigma &\rightarrow \sigma|_{K_i} \end{aligned}$$

qui est bien défini car K_i est extension normale de K_{i-1} , est surjectif car K_n est un corps de rupture, et, surtout, son noyau est $G(K_n | K_i)$, d'où l'égalité

$$G(K_n | K_{i-1}) / G(K_n | K_i) = G(K_i | K_{i-1}).$$

$xyx^{-1}y^{-1}$
facilement

Un premier bilan.

Pour une équation résoluble, on vient donc de montrer que, si le corps de base K contient les racines adéquates de l'unité, alors le corps de rupture est contenu dans une extension de K dont le groupe de Galois a la propriété suivante :

- il existe une chaîne décroissante de sous-groupes, chacun normal dans le précédent et avec un quotient abélien (même cyclique), le dernier étant l'identité.

Le groupe G possède donc la chaîne suivante :

$$G \supset G_1 \supset \dots \supset G_{n-1} \supset \text{id}, \quad \text{avec} \quad G_i/G_{i+1} \text{ abélien.}$$

Un tel groupe est dit **résoluble** (comme par hasard...).

Si le corps de base contient les racines adéquates de l'unité, alors le corps de rupture d'une équation résoluble est contenu dans une extension dont le groupe de Galois est résoluble.

Les groupes résolubles.

- Il est clair que tout groupe abélien est résoluble.
- Si p est premier, on montre que tout groupe d'ordre p^n possède un sous-groupe normal d'ordre p^{n-1} , d'où il résulte que tout groupe d'ordre puissance d'un nombre premier est résoluble.
- Les groupes symétriques de degrés 2, 3, 4, sont résolubles, des chaînes adéquates étant

$$\begin{aligned} \Sigma_2 &\supset \text{id} \\ \Sigma_3 &\supset A_3 \supset \text{id} \\ \Sigma_4 &\supset A_4 \supset K \supset \text{id} \end{aligned}$$

où K est le groupe d'ordre 4, non cyclique, formé de l'identité et des produits de couples de transpositions disjointes (voir *Le Défi algébrique*, tome I, page 330).

Par contre, pour $n \geq 5$, on montre que le seul sous-groupe propre normal de Σ_n autre que id est A_n , et aucune des deux chaînes

$$\begin{aligned} \Sigma_n &\supset \text{id} \\ \Sigma_n &\supset A_n \supset \text{id} \end{aligned}$$

ne convient, car A_n n'est pas abélien et n'a pas d'autre sous-groupe normal propre que id . Il en résulte que Σ_n n'est pas un groupe résoluble.

D'autres caractérisations des groupes résolubles sont aussi utilisées. Ainsi, on appelle **groupe dérivé** $D(G)$ du groupe G le sous-groupe engendré par les

De la ch

Pour $i =$

Inverser

montre qu

On voit
que tout q

Il en est
groupe no

La touche

Avant
améliorati

- suppr
- mont

Voyons-
1° Que
exposants
Plus pré
 m -ième de
seront des

On part

où $K(b_1, \dots)$
pour tout

$xyx^{-1}y^{-1}$. C'est le plus petit groupe tel que le quotient soit abélien : on vérifie facilement en effet :

$$G/H \text{ abélien} \Leftrightarrow H \supset D(G).$$

De la chaîne ci-dessus correspondant au groupe résoluble G on déduit

$$G_1 \supset D(G), \quad G_2 \supset D(G_1) \supset D^2(G), \dots, G_i \supset D^i(G).$$

Pour $i = n$, on trouve

$$D^n(G) = \text{id}.$$

Inversement, s'il existe $m \geq 1$ avec $D^m(G) = \text{id}$, la chaîne

$$G \supset D(G) \supset D^2(G) \supset \dots \supset D^{m-1}(G) \supset \text{id}$$

montre que G est résoluble, car les quotients sont abéliens.

Un groupe est résoluble si, et seulement si, l'un de ses dérivés successifs est réduit à l'identité.

On voit facilement que tout sous-groupe d'un groupe résoluble l'est aussi, ainsi que tout quotient, ce qui résulte de l'égalité :

$$D(G/H) = HD(G)/H.$$

Il en est donc de même de toute image homomorphique. Mieux, si H est sous-groupe normal de G , on montre :

$$G \text{ résoluble} \Leftrightarrow H \text{ et } G/H \text{ résolubles.}$$

La touche finale.

Avant d'examiner une éventuelle réciproque, on va apporter deux améliorations :

- supprimer l'hypothèse relative aux racines de l'unité
- montrer que le corps de rupture de P a lui-même un groupe de Galois résoluble.

Voyons-les successivement.

1° Que se passe-t-il si K ne contient pas les racines n_i -ième de l'unité pour les exposants n_i qui interviennent ? Tout simplement, on les adjoint.

Plus précisément, appelons m le P.P.C.M. des n_i , et ω une racine primitive m -ième de l'unité, par exemple $e^{\frac{2\pi i}{m}}$. Toutes les racines de l'unité qui interviennent seront des puissances de ω .

On part alors de notre chaîne

$$K \subset K(b_1) \subset K(b_1, b_2) \subset \dots \subset K(b_1, \dots, b_n)$$

où $K(b_1, \dots, b_n)$ est une extension normale de K contenant les racines de P et où, pour tout i , on a la relation

$$b_i^{n_i} \in K(b_1, \dots, b_{i-1}).$$

On « intercale » ω , qui est un radical relatif à K et l'on forme donc

$$K \triangleleft K(\omega) \triangleleft K(\omega, b_1) \triangleleft K(\omega, b_1, b_2) \triangleleft \cdots \triangleleft K(\omega, b_1, \dots, b_n).$$

Le dernier corps est encore extension normale de K et il contient les racines de P ; la chaîne décroissante de groupes sera (en appelant G le groupe de Galois sur K de ce dernier corps) :

$$G \supset G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \text{id}$$

avec

$$G_0 = G(K(\omega, b_1, \dots, b_n) | K(\omega))$$

$$G_i = G(K(\omega, b_1, \dots, b_n) | K(\omega, b_1, \dots, b_i)).$$

Pour tout $i \geq 1$, le quotient G_{i-1}/G_i est cyclique, car égal au groupe de Galois de $X^{n_i} - b_i^{n_i}$ sur $K(\omega, b_1, \dots, b_{i-1})$: c'est le cas ci-dessus, car le corps contient la racine ω , donc les racines n_i -ièmes de l'unité.

Reste le quotient G/G_0 , égal au groupe de Galois de $X^m - 1$ sur K , donc encore abélien comme sous-groupe du groupe multiplicatif des entiers premiers avec m modulo m .

En conclusion, même si K ne contient pas les racines de l'unité nécessaires, le corps de rupture d'une équation résoluble est contenu dans une extension normale à groupe de Galois résoluble.

2° Passons à la seconde amélioration. On sait que le corps de rupture N de P sur K est contenu dans un corps K_n , extension normale de K à groupe de Galois résoluble. Pourquoi le groupe de Galois de P sur K est-il lui-même résoluble ?

Autrement dit, dans la situation

$$K \subset N \subset K_n$$

où les extensions sont toutes normales, quelle relation y a-t-il entre $G(N|K)$ et $G(K_n|K)$?

Une fois de plus, l'homomorphisme « restriction »

$$G(K_n|K) \rightarrow G(N|K) = G(P|K)$$

$$\sigma \rightarrow \sigma|_N$$

donne la réponse : il est surjectif car K_n est un corps de rupture sur K ; dès lors $G(N|K)$, image homomorphe (donc quotient) d'un groupe résoluble, est aussi résoluble.

Énoncé de la condition nécessaire.

Les deux derniers obstacles étant levés, on peut énoncer :

Si une équation est résoluble par radicaux sur un corps, son groupe de Galois sur ce corps est résoluble.

Autrement dit :

$$P(X) = 0 \text{ résoluble sur } K \Rightarrow \text{il existe } n \geq 1 \text{ avec } D^n G(P|K) = \text{id}.$$

LE GR

Une
degré in

Une
existe u
du grot
interver
racine, c

Des exe

Le seu
l'équatio
« concre
indétern

Il suffi
 $n \geq 5$, e
permuta
théorie c
de longu

montren

Dès lo
de Galo

• Si te
conjugué
de ruptu
bonne p

• Si P
racines s
du group
 n un élé
permuta
P.P.C.M

On a 1

En effe

forme donc

$(b_1, \dots, b_n)$.

contient les racines
le groupe de Galois

)).

au groupe de Galois
le corps contient la

$m - 1$ sur K , donc
des entiers premiers

unité nécessaires, le
dans une extension

s de rupture N de P
à groupe de Galois
qui-même résoluble ?

il entre $G(N|K)$ et

ture sur K : dès lors
résoluble, est aussi

...

un corps, son groupe

$G(P|K) = \text{id}$.

Une conséquence, due au fait que le groupe symétrique n'est résoluble qu'au degré inférieur à 4.

L'équation générale de degré n n'est résoluble par radicaux que pour n inférieur à 4.

Une remarque encore : si P est irréductible sur K , il suffit de supposer qu'il existe une racine de P qui s'exprime par radicaux pour conclure à la résolubilité du groupe de Galois. En effet, en adjoignant les radicaux et racines de l'unité intervenant dans cette racine, on trouve une extension normale contenant cette racine, donc toutes les racines.

Des exemples « concrets » d'équations non résolubles.

Le seul exemple d'équation non résoluble que l'on a jusqu'à présent est celui de l'équation générale de degré supérieur à 5. On aimerait un exemple plus « concret », sur le corps $\mathbb{Q}$, c'est-à-dire faisant intervenir des nombres et non des indéterminées.

Il suffit pour cela de construire un polynôme à coefficients rationnels, de degré $n \geq 5$, et dont le groupe de Galois soit tout le groupe Σ_n ; autrement dit, toutes les permutations des racines doivent être bonnes. On utilise pour cela un résultat de théorie des groupes : le groupe Σ_n est engendré par une transposition et un cycle de longueur n ; en effet, les égalités comme

$$(1 \ 2 \ \dots \ n)(1 \ 2)(1 \ 2 \ \dots \ n)^{-1} = (2 \ 3)$$

montrent que l'on obtient toute les transpositions, donc tout le groupe Σ_n .

Dès lors, il suffit que $P \in \mathbb{Q}[X]$ soit de degré n supérieur à 5 et que son groupe de Galois contienne une transposition et un cycle de longueur n .

- Si toutes les racines de P sont réelles sauf deux, ces deux-là sont complexes conjuguées, et la conjugaison complexe fournit un $\mathbb{Q}$ -automorphisme du corps de rupture qui correspond à la transposition de ces deux racines : c'est là une bonne permutation.

- Si P est irréductible sur $\mathbb{Q}$, il est polynôme minimum de ses racines, donc ces racines sont de degré n sur $\mathbb{Q}$ et n divise le degré du corps de rupture, donc l'ordre du groupe de Galois ; si n est premier, il existe dans un groupe d'ordre multiple de n un élément d'ordre n (voir *Le Défi algébrique*, tome I, page 335) et une permutation d'ordre n premier dans Σ_n est forcément un cycle (car l'ordre est le P.P.C.M. des ordres des cycles d'une décomposition cyclique).

On a montré :

Une équation irréductible sur $\mathbb{Q}$, de degré premier supérieur à 5 et ayant toutes ses racines réelles sauf deux, n'est pas résoluble par radicaux sur $\mathbb{Q}$.

En effet, son groupe de Galois est le groupe symétrique, de degré supérieur à 5.

Un exemple plus explicite dans cette direction : on peut chercher un polynôme de degré 5, à coefficients entiers, irréductible sur $\mathbb{Q}$ et dont le graphe coupe trois fois l'axe des abscisses.

On « parachute » souvent

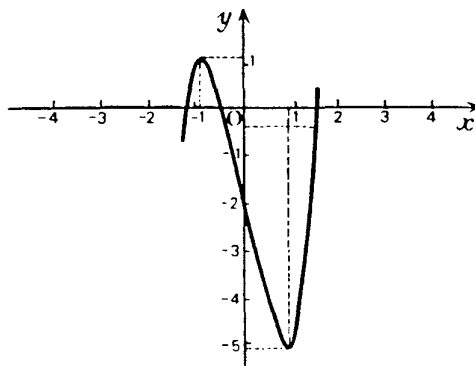
$$P = X^5 - 4X - 2.$$

Deux choses à vérifier :

- P a exactement trois racines réelles. On calcule pour cela

$$P' = 5X^4 - 4$$

qui possède deux racines réelles, $\sqrt[4]{\frac{2}{5}}$ et son opposé. Les valeurs $P(-1) = 1$ et $P(0) = -2$ donnent alors la courbe suivante :



- P est irréductible sur $\mathbb{Q}$. D'après un résultat général, un polynôme sur $\mathbb{Z}$, réductible sur $\mathbb{Q}$, serait réductible sur $\mathbb{Z}$, d'où une égalité

$$X^5 - 4X - 2 = TS$$

dans $\mathbb{Z}[X]$. On en déduit d'une part $-2 = T(0)S(0)$ et d'autre part, modulo 2, $\bar{X}^5 = \bar{T}\bar{S}$; il en résulte que $\bar{T}$ et $\bar{S}$ divisent X^5 dans $\mathbb{Z}/2[X]$, ce sont donc des puissances de X modulo 2, et les termes constants $T(0)$ et $S(0)$ sont pairs tous deux, ce qui contredit le fait que leur produit vaut -2 (on a appliqué le critère d'Eisenstein).

Les racines de $X^5 - 4X - 2$ ne peuvent pas s'exprimer à l'aide d'opérations rationnelles et d'extractions de radicaux.

En d'autres termes, on ne peut pas adjoindre à $\mathbb{Q}$ des radicaux successifs pour « englober » au bout d'un nombre fini d'opérations le corps de rupture de ce polynôme.

Un raffinement

Une propriété

Prenons
Si n est
adjoignant
 $K(\alpha^n)$. Au

on peut se
degré premier

Mais, si
Galois de
suivant qu'
groupes d'
cyclique d'
premier d'
Dans ce

Une autre

En fait,
que celle-ci

$G \cong$
équivalent à

$G \cong$
c'est-à-dire

Pour les
telle que l'
que les inc

cher un polynôme
traphe coupe trois

Un raffinement sur le groupe de Galois d'une équation résoluble.

Une remarque simple va nous permettre d'exprimer d'une autre manière la propriété du groupe de Galois d'une équation résoluble $P(X) = 0$.

Prenons un radical d'un élément de K , c'est-à-dire un α avec $\alpha^n \in K$.

Si n est égal à pq , l'extension $K(\alpha)$ s'écrit aussi $K(\alpha^p)(\alpha)$ et s'obtient donc en adjoignant à K d'abord α^p , radical de degré q sur K , puis α , radical de degré p sur $K(\alpha^p)$. Autrement dit, en amplifiant s'il le faut la chaîne

$$K \subset K_1 \subset K_2 \subset \dots \subset K_n$$

on peut supposer que chaque corps est extension du précédent par un radical de degré premier.

On l'a vu dans l'exemple de $X^4 - 2$, où au lieu de

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2}, i)$$

on pouvait prendre

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2}, i).$$

Mais, si p est premier et si K contient les racines p -ièmes de l'unité, le groupe de Galois de $K(\sqrt[p]{u})$ sur K , avec $u \in K$, est id ou C_p (groupe cyclique d'ordre p) suivant que u possède ou non une racine p -ième dans K . Dans la chaîne des sous-groupes du groupe de Galois, le quotient d'un sous-groupe par son suivant est cyclique d'ordre premier, ce qui équivaut à dire que chacun est normal d'indice premier dans le précédent, vu que C_p est le seul groupe d'ordre p .

Dans ces conditions, on peut énoncer :

Si une équation est résoluble, son groupe de Galois a une chaîne décroissante finie de sous-groupes, allant jusqu'à id , chacun normal d'indice premier dans le précédent.

Une autre caractérisation des groupes résolubles.

En fait, malgré les apparences, cette propriété n'est pas strictement plus forte que celle de groupe résoluble, elle lui est équivalente : l'existence d'une chaîne

$$G \supset G_1 \supset G_2 \dots \supset G_{n-1} \supset e \quad \text{avec} \quad G_i/G_{i+1} \text{ abélien}$$

équivaut à l'existence (*a priori* plus forte) d'une chaîne

$$G \supset H_1 \supset H_2 \dots \supset H_{m-1} \supset e \quad \text{avec} \quad H_i : H_{i+1} \text{ premier,}$$

c'est-à-dire H_i/H_{i+1} cyclique d'ordre premier.

Pour le montrer, on prendra une chaîne *maximale* du premier type, c'est-à-dire telle que l'on ne puisse intercaler aucun sous-groupe strictement, et on vérifiera que les indices sont alors forcément premiers.

Tout revient à l'implication suivante : si H est un sous-groupe normal de G , d'indice non premier, et tel que G/H soit abélien, il existe K , strictement compris entre G et H , avec $G \supset K \supset H$ (en ce cas K/H et G/K sont abéliens forcément, respectivement comme sous-groupe et quotient de G/H).

On prendra un nombre premier p divisant strictement l'indice $G : H$; il existe alors dans G/H un élément d'ordre p (voir *Le Défi algébrique*, tome I, page 335), soit la classe modulo H d'un $x \in G$. Le sous-groupe K engendré par le sous-groupe normal H et l'élément x est l'ensemble des zx^n quand z décrit H et n décrit $\mathbb{N}$.

Le fait que H soit sous-groupe propre de K résulte de $x \notin H$, et H est normal dans K car normal dans G .

D'autre part, K est sous-groupe propre de G car l'indice $G : H$ est multiple strict de l'indice $K : H = p$. Reste à montrer que K est normal dans G , donc que K contient les conjugués de x (car H est déjà stable par conjugaisons et K est engendré par H et x) ; or, si α est dans G , l'élément $\alpha x \alpha^{-1}$ est égal à x modulo H (d'après le caractère abélien de G/H), il est donc bien dans K .

Un groupe résoluble est un groupe ayant une chaîne décroissante finie de sous-groupes, allant jusqu'à id, chacun normal d'indice premier dans le précédent.

Exercices

1. On montre que si un polynôme irréductible de degré premier est résoluble, le corps de rupture est engendré par deux quelconques des racines.

En déduire que si une équation sur $\mathbb{Q}$, de degré premier, résoluble sur $\mathbb{Q}$, a deux racines réelles et est irréductible, toutes ses racines sont réelles.

Dès lors, une équation irréductible sur $\mathbb{Q}$ de degré premier supérieur à 5 n'est pas résoluble si elle a exactement trois racines réelles.

2. Une équation de degré 3 à coefficients réels est, on l'a vu, résoluble. Même si les racines sont réelles, c'est-à-dire si le discriminant est positif, les formules obtenues font intervenir des nombres non réels (comme j). N'y-a-t-il pas de formules purement réelles donnant les racines réelles d'une équation réelle de degré 3 (comme c'est le cas au degré 2) ?

On montrera que non, comme conséquence du résultat suivant : si P est un polynôme irréductible de degré impair sur le corps K réel et si son corps de rupture est engendré par une racine, alors aucune adjonction de radicaux réels ne réduit le groupe de Galois (on appliquera au degré 3 en prenant pour K le corps engendré par les racines carrées du discriminant et les coefficients, car alors toute racine est primitive dans le corps de rupture).

On commencera par montrer que P possède une racine réelle x_1 , donc que son corps de rupture $K(x_1)$ est réel et l'on supposera que le radical $\sqrt[p]{c}$, réel et avec p premier, réduit le groupe de Galois à un sous-groupe d'indice $m \geq 2$.

On

• m

• le

au

• l'é

• l'e

• l'e

ru

• co

co

3. Mor

On

décr

« sui

grou

Pour

upe normal de G ,
strictement compris
béliens forcément,

ice $G : H$; il existe
tome I, page 335),
endré par le sous-
ad z décrit H et n

H , et H est normal

$G : H$ est multiple
l dans G , donc que
jugaisons et K est
égal à x modulo H
 K .

haîne décroissante
in normal d'indice

est résoluble, le corps

soluble sur $\mathbb{Q}$, a deux
elles.
upérieur à 5 n'est pas

soluble. Même si les
es formules obtenues
t-il pas de formules
on réelle de degré 3

suivant : si P est un
son corps de rupture
eux réels ne réduit le
 K le corps engendré
alors toute racine est

elle x_1 , donc que son
cal $\sqrt[p]{c}$, réel et avec p
lice $m \geq 2$.

On montrera successivement :

- m est impair ;
- le polynôme $X^p - c$ est irréductible sur K (on montrera que K n'en contient aucune racine);
- l'élément $\sqrt[p]{c}$ est de degré p sur K ;
- l'entier m divise p ;
- l'entier m est égal à p , donc $\sqrt[p]{c}$ est une irrationnelle naturelle (dans le corps de rupture);
- comme $\sqrt[p]{c}$ est une irrationnelle naturelle, le corps de rupture $K(x_1)$, qui la contient, contient ses conjugués qui sont non réels : contradiction.

3. Montrer qu'un groupe résoluble G est caractérisé par la condition suivante. On forme une « série de composition » en écrivant une suite strictement décroissante de sous-groupes, chacun normal maximal dans le précédent, puis la « suite des indices » de la série, c'est-à-dire la suite des indices de chaque sous-groupe dans le précédent. Alors

G résoluble $\Leftrightarrow$ la suite des indices est formée de nombres premiers.

Pour les groupes symétriques, les suites que l'on trouve sont

$$\begin{array}{lll} 2 & \text{pour} & \Sigma_2 \\ 2, 3 & \text{pour} & \Sigma_3 \\ 2, 3, 2, 2 & \text{pour} & \Sigma_4 \\ 2, \frac{n!}{2} & \text{pour} & \Sigma_n \ (n \geq 5). \end{array}$$

La caractérisation des équations résolubles

Pour que le résultat soit complet, il reste à voir la réciproque de la condition nécessaire ci-dessus : si le groupe de Galois de P sur K est un groupe résoluble, l'équation $P(X) = 0$ est résoluble sur K , c'est-à-dire que ses racines s'expriment algébriquement à l'aide de K .

On a le choix entre les trois définitions suivantes d'un groupe résoluble (on a montré leur équivalence) :

- il existe un entier $n \geq 1$ avec $D^n G = \text{id}$, c'est-à-dire que l'un des dérivés successifs de G est réduit à l'identité ;

- il existe une chaîne de sous-groupes

$$G \supset G_1 \supset \cdots \supset G_{m-1} \supset \text{id}$$

avec G_i/G_{i+1} abélien ;

- il existe une chaîne de sous-groupes

$$G \supset G_1 \supset \cdots \supset G_{q-1} \supset \text{id}$$

avec $G_i : G_{i+1}$ premier (donc G_i/G_{i+1} cyclique d'ordre premier).

C'est cette dernière caractérisation que l'on va prendre.

La position du problème.

On part donc de $P \in K[X]$, le groupe de Galois $G(P|K)$ ayant une chaîne finie décroissante G_i de sous-groupes, allant jusqu'à id et chacun normal d'indice premier dans le précédent.

Comment peut-on alors « monter » du corps K à un corps contenant les racines de P , par adjonctions successives de radicaux ? La chaîne croissante de corps sera celle des corps fixes : à tout G_i correspond le corps K_i formé par les points du corps de rupture fixes par G_i . La suite des K_i est croissante, le dernier, ou corps fixe par id , est le corps de rupture. Tout reste à voir si chaque K_i est extension par radical du précédent.

Un premier pas

On est alors donné, on prend le groupe de Galois de P sur K et l'adjonction d'un radical comme conséquence.

Appelons N le groupe de Galois de la

$G(I)$

C'est là un cas particulier (p. 215) :

- le groupe H est normal dans G que l'indice p divise l'ordre de G ;
- l'extension $K(H)$ est une extension caractéristique normale de K par conjugaison ;

On peut donc

On est alors en présence d'un premier, c'est-à-dire d'un groupe cyclique.

Les extensions cycliques

De manière générale, le groupe de Galois

U
l'
S
d

Le problème est de savoir si, en fait, dans n'importe quel cas, mais seulement à l'aide de radicaux. Partons donc

Un premier pas.

On est alors amené à poser le problème suivant : le polynôme $P \in K[X]$ étant donné, on prend un sous-groupe H , normal d'indice premier p , du groupe de Galois de P sur K . Que peut-on dire du corps fixe ? Se déduit-il de K par adjonction d'un radical ? C'est évidemment ce que l'on souhaiterait pour en tirer comme conséquence la réciproque du chapitre précédent.

Appelons N le corps de rupture de P sur K , et N_H le corps fixe par H . On est en présence de la situation

$$G(P|K) = G(N|K) \supset H \quad \text{avec} \quad G(P|K) : H = p$$

C'est là un cas particulier de correspondance de Galois : on a montré (voir p. 215) :

- le groupe H est le groupe de Galois de P sur le corps fixe N_H , d'où il résulte que l'indice p de H dans $G(N|K)$ est égal au degré de N_H sur K ;
- l'extension N_H de K est normale (donc c'est un corps de rupture), car le caractère normal de H comme sous-groupe de $G(N|K)$ entraîne la saturation de N_H par conjugaisons ; le groupe de Galois de N_H sur K est le groupe quotient de $G(P|K)$ par H .

On peut donc « raffiner » la situation :

$$K \triangleleft N_H \triangleleft N \quad \text{avec} \quad N_H : K = p.$$

On est alors naturellement amené à étudier les extensions normales de degré premier, c'est-à-dire celles dont le groupe de Galois est d'ordre premier (et alors forcément cyclique).

Les extensions cycliques.

De manière générale, on appelle **extension cyclique** de K toute extension dont le groupe de Galois sur K est cyclique.

Un exemple a déjà été vu : si K contient les racines n -ièmes de l'unité, alors $K(\sqrt[n]{a})$ est extension cyclique de K (voir p. 153). Si n est premier, il suffit d'ailleurs que a n'ait pas de racine n -ième dans K pour que $X^n - a$ soit irréductible.

Le problème est, en gros : toute extension cyclique est-elle de ce type ?

En fait, dans notre cas, on ne s'intéresse pas à *toutes* les extensions cycliques, mais seulement à celles qui sont *normales* de degré *premier*.

Partons donc de L , extension normale de degré p premier sur K .

stérisation
résolubles

que de la condition
n groupe résoluble,
racines s'expriment

upe résoluble (on a

ue l'un des dérivés

emier).

ant une chaîne finie
un normal d'indice

corps contenant les
chaîne croissante de
rps K_i formé par les
croissante, le dernier,
oir si chaque K_i est

On note successivement :

- L est bien une extension cyclique de K, car son groupe de Galois sur K est d'ordre p , donc cyclique, égal à C_p ;
- Tout élément de $L \setminus K$ est de degré p sur K (par multiplicativité des degrés), donc primitif sur L et, par suite, L est corps de rupture du polynôme minimum d'un tel élément;
- L étant corps de rupture, sur K, du polynôme $P \in K[X]$ irréductible de degré p , le groupe de Galois de P sur K est engendré par une permutation cyclique de longueur p des racines de P (car l'ordre d'une permutation est le P.P.C.M. des longueurs de sa décomposition cyclique); on peut supposer les racines $(x_1, \dots, x_p)$ de P numérotées de manière que $G(P|K)$ soit engendré par le cycle $\sigma = (1 \ 2 \ \dots \ p)$.

On cherche un élément primitif « sympathique », de préférence un radical par rapport à K (c'est-à-dire ayant une de ses puissances dans K).

Or, tout élément de L s'écrit

$$u_1 x_1 + \dots + u_p x_p$$

avec les u_i dans K et, dans cette expression, il est équivalent d'effectuer la permutation σ sur les x_i ou la permutation σ^{-1} sur les u_i . Mais σ^{-1} transforme u_i en u_{i-1} et un « bon candidat » correspondra au choix, pour les u_i , de la suite des racines p -ièmes de l'unité.

Supposons donc, pour commencer, que K contient une racine p -ième de l'unité autre que 1, soit ω . Alors K contient le corps de rupture de $X^p - 1$, la suite des p racines p -ièmes de l'unité étant $(1, \omega, \omega^2, \dots, \omega^{p-1})$. On va prendre $u_i = \omega^{i-1}$, c'est-à-dire considérer l'élément

$$y = x_1 + \omega x_2 + \dots + \omega^{p-1} x_p \in L.$$

Si l'on applique la permutation $\sigma = (1 \ 2 \ \dots \ p)$ aux x_i , on a vu qu'il reste $\sigma y = \omega^{-1} y$. Il en résulte que y^p est fixe par σ , donc par les puissances de σ , donc par le groupe de Galois de P sur K. Mais alors y^p est dans le corps de base K et y est bien un radical par rapport à K.

Reste à voir si y est élément primitif de L, donc si y est hors de K (car tout élément de $L \setminus K$ est de degré p sur K, donc primitif). Or, on écrit :

$$y \in K \Leftrightarrow \sigma y = y \Leftrightarrow \omega^{-1} y = y \Leftrightarrow y = 0$$

et tout revient à montrer que, pour au moins une des $(p-1)$ valeurs de ω , l'élément y correspondant est non nul.

Appelons pour cela $y(\omega)$ l'élément

$$x_1 + \omega x_2 + \dots + \omega^{p-1} x_p;$$

les autres sont

$$y(\omega^2), y(\omega^3), \dots, y(\omega^{p-1})$$

et l'on veut montrer qu'au moins l'un d'entre ces $(p-1)$ éléments est non nul. On calcule pour cela

$$y(1) + y(\omega) + \dots + y(\omega^{p-1})$$

$$= p x_1 + x_2 \sum_{i=0}^{p-1} \omega^i + x_3 \sum_{i=0}^{p-1} \omega^{2i} + \dots + x_p \sum_{i=0}^{p-1} \omega^{(p-1)i}.$$

La son

Or, $y(1)$ étaient nu polynôme

Résumo normale c

Plus pré sont ses $x_1 + \omega x_2$ l'extensior

La conclus

Revenor est suppos On va aj tout de sui Galois H d donc encoi

avec $p_i = 1$

où L conti

Mais K_i H_i/H_{i+1} , cy divise celui

l'identité (c s'écrit $K_i(a$ binôme de

Les racir racine de Récapituloi

C'est là l

de Galois sur K est

cativité des degrés),
polynôme minimum

$[X]$ irréductible de
r une permutation
permutation est le
i peut supposer les
soit engendré par le

ence un radical par
 K).

alent d'effectuer la
is σ^{-1} transforme u_i
les u_i , de la suite des

ine p -ième de l'unité
 $p - 1$, la suite des p
prendre $u_i = \omega^{i-1}$,

on a vu qu'il reste
puissances de σ , donc
corps de base K et y

hors de K (car tout
on écrit :

$r = 0$

$- 1$) valeurs de ω ,

ients est non nul. On

$$\dots + x_p \sum_{i=0}^{p-1} \omega^{(p-1)i}.$$

La somme des p racines p -ièmes de l'unité étant nulle, il reste

$$y(\omega) + \dots + y(\omega^{p-1}) = px_1 - y(1).$$

Or, $y(1)$ est la somme des x_i , elle est dans K et, si tous les $y(\omega^j)_{j=1, \dots, p-1}$ étaient nuls, alors x_1 serait dans K , ce qui contredit le fait que x_1 est racine du polynôme P irréductible sur K .

Résumons : si K contient les racines p -ièmes de l'unité, alors toute extension normale de degré premier de K est une extension par radical.

Plus précisément, si x_1 est dans cette extension et hors de K et si $x_1, x_2, \dots, x_p$ sont ses conjugués, il existe une racine p -ième ω de l'unité telle que $x_1 + \omega x_2 + \dots + \omega^{p-1} x_p$ soit non nul; c'est alors un élément primitif de l'extension et c'est une racine p -ième d'un élément de K .

On a déjà utilisé cette propriété au degré 3 (voir p. 57), en associant aux racines x_1, x_2, x_3 de $X^3 + pX + q$ l'élément $x_1 + jx_2 + j^2x_3$.

La conclusion.

Revenons maintenant à notre polynôme $P \in K[X]$ dont le groupe de Galois G est supposé résoluble.

On va appeler n l'ordre de G (ou degré du corps de rupture de P) et adjoindre tout de suite à K une racine primitive n -ième de l'unité, soit ω . Le groupe de Galois H de P sur $K(\omega)$ est un sous-groupe du groupe de Galois de P sur K , il est donc encore résoluble. On écrit la chaîne

$$G(P|K(\omega)) = H \supset H_1 \supset \dots \supset \{id\}$$

avec $p_i = H_i : H_{i+1}$ premier, puis la suite des corps fixes

$$K(\omega) \triangleleft K_1 \triangleleft \dots \triangleleft L$$

où L contient le corps de rupture de P sur K .

Mais K_{i-1} est extension cyclique de K_i , puisque son groupe de Galois est H_i/H_{i+1} , cyclique d'ordre p_i . Comme p_i divise n (car p_i divise l'ordre de H_i , qui divise celui de H , donc celui de G), le corps K_i contient les racines p_i -ièmes de l'identité (car $\omega^{\frac{n}{p_i}}$ est racine primitive p_i -ième) et, d'après ce qui précède, K_{i+1} s'écrit $K_i(a_i)$, avec $a_i^{p_i} \in K_i$: il y a un élément primitif racine d'une équation binôme de degré p_i .

Les racines de P sont alors contenues dans $K(\omega, a_1, a_2, \dots)$, où ω est une racine de l'unité et chaque a_i un radical relatif à $K(\omega, a_1, \dots, a_{i-1})$. Récapitulons :

Les racines d'une équation s'expriment algébriquement sur un corps si, et seulement si, le groupe de Galois sur ce corps est résoluble.

C'est là le « couronnement » de la théorie de Galois.

Ainsi, si un polynôme a un groupe de Galois abélien ou d'ordre puissance d'un nombre premier, ses racines s'expriment algébriquement à l'aide des éléments du corps de base.

Ceci dit, il ne faut pas surestimer le côté « pratique » du résultat, vu la difficulté de calculer explicitement le groupe de Galois d'une équation concrète prise « au hasard » (voir p. 140).

Le raffinement suprême.

En fait, si l'on réfléchit de près à ce qu'est un radical, on voit apparaître une séparation entre « vrais » et « faux » radicaux.

Ainsi, une racine cubique de l'unité autre que 1 peut s'écrire $\sqrt[3]{1}$, elle peut aussi s'écrire $\frac{-1 + \sqrt{-3}}{2}$. La différence, c'est que la seconde écriture donne le résultat cherché quelle que soit la racine carrée de -3 choisie, alors que la première écriture inclut 1 dont on ne veut pas.

En d'autres termes, si l'on veut résoudre l'équation $1 + X + X^2 = 0$, ses solutions seront *certaines* des trois quantités désignées par le symbole $\sqrt[3]{1}$, mais ce seront *toutes* les deux quantités désignées par le symbole $\frac{-1 + \sqrt{-3}}{2}$, et la raison profonde est la suivante : le radical $\sqrt[3]{1}$ correspond à l'équation binôme $X^3 - 1$, réductible sur $\mathbb{Q}$, alors que le radical $\sqrt{-3}$ correspond, lui, à $X^2 + 3$, irréductible sur $\mathbb{Q}$.

Ceci dit, partons d'une équation $P(X) = 0$ sur le corps de base K . S'il y a une racine qui s'exprime par radicaux, chaque radical qui intervient a plusieurs valeurs possibles, et il serait souhaitable que l'on tombe sur une racine de P quels que soient les choix faits pour les divers radicaux (ainsi, $\sqrt[3]{1}$ ne donne pas toujours une racine de $1 + X + X^2$, seuls deux des trois choix sont bons).

Comment faire pour s'assurer que tout se passe bien ainsi ? Il suffira que, chaque fois qu'intervient un radical $\sqrt[n]{a}$, l'équation binôme correspondante $X^n - a$ soit irréductible sur le corps L engendré par les radicaux antérieurement adjoints. En ce cas en effet, les diverses valeurs de $\sqrt[n]{a}$ sont conjuguées sur L , donc se correspondent dans des L -isomorphismes, que l'on peut prolonger en des L -isomorphismes (donc *a fortiori* des K -isomorphismes) des extensions postérieures : dès lors, si l'une des déterminations de $\sqrt[n]{a}$ donne une racine de P , il en sera de même des autres. Bien entendu, si $\sqrt[n]{a}$ apparaît à divers endroits dans l'expression, il prend partout la même valeur.

Par exemple, un symbole comme $\sqrt{\frac{-1 + \sqrt{-3}}{2}}$ désigne quatre nombres complexes. Si j est une racine primitive cubique de 1, ces quatre nombres sont $j, j^2, -j, -j^2$.

Pour faire
est un **radic**
sur M .

Un cas pa
alors $\sqrt[n]{a}$ es

On aimer
 $P \in K[X]$, n
s'arrangeant

Or, si l'or
adjointe une
Galois). les a
dans le corp
sont pas, et
première ad

D'où la q
successifs irr

Toute raci
contentera d
formules rela

pour $m =$

pour $m =$

pour $m =$

s abélien ou d'ordre
racines s'expriment
rps de base.

sultat, vu la difficulté
concrète prise « au

voit apparaître une

re $\sqrt[3]{1}$, elle peut aussi

le écriture donne le

choisie, alors que la

+ $X + X^2 = 0$, ses
le symbole $\sqrt[3]{1}$, mais
 $\frac{-1 + \sqrt{-3}}{2}$, et la

à l'équation binôme
spond, lui, à $X^2 + 3$,

e base K . S'il y a une
intervient a plusieurs
une racine de P quels
i, $\sqrt[3]{1}$ ne donne pas
choix sont bons).

ainsi ? Il suffira que,
ôme correspondante
caux antérieurement
onjuguées sur L , donc
ut prolonger en des
nes) des extensions
nne une racine de P , il
divers endroits dans

$\frac{-1 + \sqrt{-3}}{2}$ désigne

ine primitive cubique
- j^2 .

Or, les deux premiers sont racines de $1 + X + X^2$, les deux
derniers de $1 - X + X^2$.

En d'autres termes, écrire une racine de $1 - X + X^2$ comme

$\sqrt{\frac{-1 + \sqrt{-3}}{2}}$ est abusif, car seuls deux des quatre choix

conviennent, et ceci est dû au fait que $X^2 - \frac{-1 + \sqrt{-3}}{2}$ n'est

pas irréductible sur $\mathbb{Q}(\sqrt{-3})$, car on écrit

$$X^2 - \frac{-1 + \sqrt{-3}}{2} = \left(X - \frac{-1 - \sqrt{-3}}{2}\right) \left(X + \frac{-1 - \sqrt{-3}}{2}\right).$$

Par contre, si l'on dit que $\frac{1 + \sqrt{-3}}{2}$ est racine de $1 - X + X^2$,

ici il n'y a aucun doute car les deux choix des racines carrées de
- 3 donnent les deux racines de $1 - X + X^2$.

Pour faire la distinction, on dira qu'un radical $\sqrt[n]{a}$ d'un élément a d'un corps M
est un **radical irréductible** sur M quand le polynôme $X^n - a$ est irréductible
sur M .

Un cas particulier : si p est premier et si $a \in M$ n'a pas de racine p -ième dans M ,
alors $\sqrt[p]{a}$ est un radical irréductible sur M .

On aimerait alors voir s'il est possible d'arriver aux racines du polynôme
 $P \in K[X]$, non seulement en adjoignant à K des radicaux successifs mais en
s'arrangeant pour qu'à chaque pas le radical adjoit soit *irréductible*.

Or, si l'on examine la démonstration précédente, on s'aperçoit qu'une fois
adjoite une racine n -ième primitive de l'unité (n étant l'ordre du groupe de
Galois), les autres radicaux adjoints sont tous d'indice premier : ou bien ils sont
dans le corps précédent, et alors leur adjonction ne change rien, ou bien ils n'y
sont pas, et alors ce sont des radicaux irréductibles. Tout réside donc dans la
première adjonction, celle de ω .

D'où la question : les racines de l'unité s'expriment-elles à l'aide de radicaux
successifs irréductibles ?

Toute racine de l'unité est racine primitive pour un certain indice m , on se
contentera donc du problème pour les racines primitives. On a déjà montré les
formules relatives à plusieurs valeurs de m :

pour $m = 3$ c'est $\frac{-1 + \sqrt{-3}}{2}$;

pour $m = 4$ c'est $\sqrt{-1}$;

pour $m = 5$ on a calculé $\frac{-1 + \sqrt{5}}{4} + \frac{1}{2} \sqrt{\frac{-5 - \sqrt{5}}{2}}$;

pour $m = 6$ c'est $\frac{1 + \sqrt{-3}}{2}$;

pour $m = 7$ l'expression était plus compliquée

$$\frac{1}{3} \left(\frac{-1 + \sqrt{-7}}{2} + \sqrt[3]{7 - \frac{3}{2}\sqrt{21} - \frac{1}{2}\sqrt{-7}} + \frac{\sqrt{-7}}{\sqrt[3]{7 - \frac{3}{2}\sqrt{21} - \frac{1}{2}\sqrt{-7}}} \right) ;$$

pour $m = 8$ on trouve $\frac{1 + \sqrt{-1}}{\sqrt{2}}$.

Dans ce dernier exemple, $\sqrt{-7}$ peut prendre deux valeurs distinctes, ainsi que $\sqrt{21}$, alors que la racine cubique en prend trois, ce qui donne *a priori* douze racines primitives septième de l'unité au lieu de six. En fait, on ne trouve que six valeurs, car changer le signe de $\sqrt{21}$ et pas celui de $\sqrt{-7}$ revient à échanger les deux derniers termes sans toucher au premier.

Ceci dit, pour montrer que toute racine primitive de l'unité s'exprime à l'aide de radicaux irréductibles, on vérifie successivement :

- si s et t sont premiers entre eux, le produit d'une racine primitive s -ième par une racine primitive t -ième est une racine primitive st -ième ; le problème se ramène donc au cas où l'indice est puissance d'un nombre premier ;
- si p est premier, une racine primitive p^2 -ième de l'unité est une racine p -ième d'une racine p -ième primitive de l'unité, donc s'exprimera à l'aide de radicaux successifs irréductibles si cette dernière s'exprime ainsi ; de même pour les racines p^3 -ièmes, p^4 -ièmes, etc., donc tout se réduit au cas où l'indice est premier ;
- pour montrer que toute racine primitive p -ième de l'unité s'exprime à l'aide de radicaux successifs irréductibles, on remarque qu'une telle racine ω_p est de degré $p-1$ et le groupe de Galois du polynôme minimum $1 + X + \dots + X^{p-1}$ est cyclique d'ordre $p-1$ (voir p. 152) ; on décompose alors $p-1$ en facteurs premiers, soit $p-1 = p_1^{n_1} \dots p_r^{n_r}$, d'où la chaîne de sous-groupes

$$C_{p_1} \triangleleft C_{p_1^{n_1}} \triangleleft \dots \triangleleft C_{p_1^{n_1} p_2} \triangleleft C_{p_1^{n_1} p_2^{n_2}} \triangleleft \dots \triangleleft C_{p-1}$$

qui donne ω_p à l'aide de radicaux d'ordre $p_1, \dots, p_r$ et des racines p_1 -ième, $\dots, p_r$ -ième de l'unité. Il suffit alors de faire une récurrence : si les racines primitives q -ièmes, pour q premier strictement inférieur à p , s'expriment par radicaux successifs irréductibles, il en est de même des racines primitives p -ièmes.

Dans ces conditions, on peut énoncer le résultat « maximum » suivant :

Si le groupe de Galois d'un polynôme est résoluble, toute racine s'exprime à l'aide de radicaux successifs à partir du corps de base, de manière que dans une telle expression tout choix des valeurs des différents radicaux donne une racine.

Exercices.

1. Si un mêm
On j
d'un
corr
de a

2. Soit

Si n
géné

grou
etc.,

p_1, p_2

Conc
 p_1 -ième

En p
radic
non (

3. En s'i
corps
par o
l'unit

On m
ième

On co
degré

4. Une é
abélie

Mont
ième
degré

On ut
que, p
montr
en un
permu

Si α es
polyn

Exercices.

1. Si une racine d'une équation *irréductible* peut s'exprimer par radicaux, il en est de même de toutes et l'équation est résoluble.
On pourra considérer les radicaux intervenant successivement dans l'expression d'une racine et, à chaque stade, adjoindre toutes les racines de l'équation binôme correspondante $X^p - a$ et celles des équations $X^p - a_i$ où les a_i sont les conjugués de a par rapport au corps de base.

2. Soit P un polynôme dont le groupe de Galois est cyclique d'ordre n .

Si $n = p_1^{r_1} \dots p_s^{r_s}$ est la décomposition de n en facteurs premiers, et si σ est générateur du groupe de Galois, montrer que l'on peut réduire successivement le groupe de Galois au sous-groupe engendré par σ^{p_1} , puis par $\sigma^{p_1^{r_1}}$, $\sigma^{p_2^{r_2}}$, etc., ceci par adjonctions successives de racines de l'unité et de radicaux de degrés $p_1, p_2, \dots$.

Conclure que l'équation $P = 0$ est résoluble par des extractions de racines p_1 -ièmes, p_2 -ièmes, ..., p_s -ièmes.

En particulier, pour p premier, toute racine p -ième de l'unité s'exprime à l'aide de radicaux d'ordres inférieurs à $(p - 1)$. Étendre au cas où p est arbitraire, premier ou non (on pourra commencer par le cas où p est puissance d'un nombre premier).

3. En s'inspirant de la méthode utilisée pour les extensions cycliques, on partira d'un corps de rupture L sur K dont le groupe de Galois est cyclique d'ordre n engendré par σ . A partir d'un élément primitif θ de l'extension et d'une racine n -ième de l'unité ω autre que 1 (en supposant que K contient ces racines), on étudiera

$$\alpha = \theta + \omega^{-1}\sigma(\theta) + \dots + \omega^{-(n-1)}\sigma^{n-1}(\theta).$$

On montrera que l'on peut choisir ω pour que α soit non nul et qu'en ce cas α est élément primitif de L sur K et possède une puissance n -ième dans K .

On conclura que L est corps de rupture d'une équation binôme irréductible de degré n sur K .

4. Une équation **abélienne** est une équation irréductible dont le groupe de Galois est abélien. Une telle équation est résoluble.

Montrer qu'une équation abélienne est normale, c'est-à-dire que toute racine est élément primitif du corps de rupture (ou encore : le degré du corps de rupture est le degré de l'équation).

On utilisera pour cela le fait que le groupe de Galois est abélien et transitif, donc que, pour tout élément de ce groupe autre que l'identité, aucune racine n'est fixe ; on montrera alors qu'il existe une seule permutation transformant un élément donné en un autre et on en déduira que l'ordre d'un groupe abélien transitif de permutations de p éléments est égal à p , ce qui impliquera le résultat cherché.

Si α est une racine, la suite des racines s'écrit $\alpha, \varphi_2(\alpha), \dots, \varphi_n(\alpha)$, où les φ_i sont des polynômes sur le corps de base. Vérifier

$$\varphi_i \varphi_j(\alpha) = \varphi_j \varphi_i(\alpha).$$

$$\left(\frac{-7 \pm \sqrt{49 - 4 \cdot 21 \cdot \frac{1}{2} \sqrt{-7}}}{2} \right);$$

rs distinctes, ainsi
nne *a priori* douze
on ne trouve que
revient à échanger

exprime à l'aide de

imitive s -ième par
; le problème se
premier ;

une racine p -ième
l'aide de radicaux
ne pour les racines
e est premier ;

s'exprime à l'aide
e racine ω_p est de
 $1 + X + \dots + X^{p-1}$
; $p - 1$ en facteurs
oupes

$$< C_{p-1}$$

, et des racines
réurrence : si les
ur à p , s'expriment
racines primitives

um » suivant :

oluble, toute racine
ir du corps de base,
hoix des valeurs des

Constructions à la règle et au compas : la solution

Le problème de la constructibilité à la règle et au compas d'un point du plan à partir d'une partie donnée P est le premier problème que l'on a posé. Il se ramène, en supposant que P contient 1 et est symétrique par rapport à l'axe réel, à la détermination de la saturation par racines carrées du corps $\mathbb{Q}(P)$ engendré par P (voir p. 17).

La condition nécessaire.

Le critère d'appartenance au plus petit corps contenant $\mathbb{Q}(P)$ et saturé par racines carrées (c'est-à-dire dans lequel tout élément est un carré) est le suivant :

- un point est constructible à partir de P si, et seulement si, il appartient à un corps déduit de $\mathbb{Q}(P)$ par des extensions quadratiques successives, en nombre fini.

Comme chaque extension quadratique double le degré, un tel point appartient à un corps dont le degré sur $\mathbb{Q}(P)$ est une puissance de 2 ; le point lui-même a alors pour degré une puissance de 2.

Le degré de tout nombre constructible à partir d'une partie est une puissance de 2 sur le corps engendré par cette partie.

Tout nombre constructible à partir de P doit donc être racine d'un polynôme irréductible sur $\mathbb{Q}(P)$ de degré puissance de 2.

C'est là une condition nécessaire, mais non suffisante.

Ainsi, on a vu que les réponses négatives à la duplication du cube ou la trisection de l'angle de 60° correspondent aux faits que $\sqrt[3]{2}$ est de degré 3 sur $\mathbb{Q}$, ainsi que $e^{\frac{2i\pi}{18}}$ sur $\mathbb{Q}(e^{\frac{2i\pi}{6}}) = \mathbb{Q}(j)$ (voir p. 93).

La réponse négative à la quadrature du cercle est, elle, encore plus flagrante : π n'est même pas algébrique sur $\mathbb{Q}$.

On énoncera en tout cas :

Si un nombre est racine d'une équation de degré non puissance de 2, irréductible sur un sous-corps de $\mathbb{C}$, il n'est pas constructible sur ce sous-corps.

Si le degré est une puissance de 2, on ne peut rien dire *a priori*.

CONSTRUCTI

La trisection d

De même ma
à la règle et au
 $X^3 - e^{i\theta}$ ait un

Parfois, on r
partir de $\cos \theta$.

Or l'égalité

D'où les deu

• $4X^3 - 3X$
 $\cos \frac{\theta}{3}$ est soit
constructible ca

• $4X^3 - 3X$
(car de degré 3 s
non constructib

Notons d'aill

Construction à l

En partant d'u
de z à partir de
déduite de K
symétrique par

La traduction
sur K , dont le gr
d'indice 2 dans le
ce groupe doit é

La trisection de l'angle.

De même manière générale, trisecter un angle θ signifie étudier la construction à la règle et au compas de $e^{i\frac{\theta}{3}}$ à partir de 1 et $e^{i\theta}$. Pour cela, il faut et il suffit que $X^3 - e^{i\theta}$ ait une racine dans $\mathbb{Q}(e^{i\theta})$, car sinon $e^{i\frac{\theta}{3}}$ est de degré 3 sur ce corps.

Parfois, on reste dans le domaine réel; on cherche alors à construire $\cos \frac{\theta}{3}$ à partir de $\cos \theta$.

Or l'égalité $4 \cos^3 \frac{\theta}{3} - 3 \cos \frac{\theta}{3} = \cos \theta$ montre que $\cos \frac{\theta}{3}$ est racine de

$$4X^3 - 3X - \cos \theta \in \mathbb{Q}(\cos \theta)[X].$$

D'où les deux cas :

- $4X^3 - 3X - \cos \theta$ a une racine dans $\mathbb{Q}(\cos \theta)$: il est alors réductible, donc $\cos \frac{\theta}{3}$ est soit dans $\mathbb{Q}(\cos \theta)$, soit de degré 2 sur $\mathbb{Q}(\cos \theta)$ et, en tout cas, constructible car s'exprimant avec une racine carrée;

- $4X^3 - 3X - \cos \theta$ n'a pas de racine dans $\mathbb{Q}(\cos \theta)$: il est alors irréductible (car de degré 3 sans facteur de degré 1) et $\cos \frac{\theta}{3}$ est de degré 3 sur $\mathbb{Q}(\cos \theta)$, donc non constructible.

On peut trisecter à la règle et au compas l'angle θ si, et seulement si, le polynôme $4X^3 - 3X - \cos \theta$ a une racine dans $\mathbb{Q}(\cos \theta)$.

Notons d'ailleurs que, si $\cos \theta$ est rationnel, alors $\mathbb{Q}(\cos \theta)$ est égal à $\mathbb{Q}$.

On retrouve l'impossibilité de trisecter un angle de 60° en vérifiant qu'aucun rationnel n'est racine de

$$4X^3 - 3X - \frac{1}{2}.$$

Construction à la règle et au compas : la condition définitive.

En partant d'un sous-corps K de $\mathbb{C}$, on a vu que la condition de constructibilité de z à partir de K équivaut à l'existence d'une extension de K contenant z et déduite de K par extensions quadratiques successives (en supposant K symétrique par rapport à l'axe réel).

La traduction en terme de groupes de Galois part du polynôme minimum de z sur K , dont le groupe de Galois doit posséder une chaîne de sous-groupes chacun d'indice 2 dans le précédent (tout sous-groupe d'indice 2 est normal) : l'ordre de ce groupe doit être puissance de 2.

Inversement, si le groupe de Galois est d'ordre puissance de 2, il possède un sous-groupe d'indice 2 (voir *Le Défi algébrique*, tome I, page 338) donc une telle chaîne, à partir de laquelle on déduit une suite croissante d'extensions quadratiques successives de K jusqu'à englober z .

Un nombre est constructible à la règle et au compas à partir d'un corps K si, et seulement si, le groupe de Galois de son polynôme minimum est d'ordre puissance de 2, ce qui signifie que le corps de rupture de son polynôme minimum a pour degré une puissance de 2.

Cette condition entraîne que le degré du polynôme minimum, qui est le degré de z , divise une puissance de 2, donc soit puissance de 2. Mais ici la condition est nécessaire et suffisante.

Ainsi, si z a un polynôme minimum de degré 4 sur $\mathbb{Q}$, il s'exprime algébriquement sur $\mathbb{Q}$ (voir p. 65), mais en général à l'aide de radicaux de degrés 2 et 3 et, si l'un de ces derniers intervient, z n'est pas constructible.

On a vu par exemple que l'ordre du groupe de Galois du polynôme irréductible $X^4 + X + 1$ sur $\mathbb{Q}$ est divisible par 3 (voir p. 204); il en résulte que, bien que l'équation soit résoluble par radicaux et soit de degré puissance de 2, aucune des racines n'est constructible à partir de $\mathbb{Q}$ à la règle et au compas.

Par contre, pour le polynôme cyclotomique

$$1 + X + X^2 + X^3 + X^4 = \frac{X^5 - 1}{X - 1}$$

son groupe de Galois sur $\mathbb{Q}$ est, on l'a vu, cyclique d'ordre 4. Donc $e^{\frac{2i\pi}{5}}$, qui en est une racine, est constructible à la règle et au compas : c'est le résultat concernant le pentagone régulier (voir p. 229).

Construction d'un polygone régulier.

La construction à la règle et au compas d'un polygone régulier de n côtés correspond à la construction d'un angle de $\frac{2\pi}{n}$, donc elle dépend du groupe de Galois du polynôme minimum de $\omega_n = e^{\frac{2i\pi}{n}}$, sur le corps de base $\mathbb{Q}$ si l'on part des points 0 et 1.

Ce polynôme Φ_n est appelé le polynôme cyclotomique d'indice n , ses racines sont les racines primitives n -ièmes de l'unité, donc les $e^{\frac{2ik\pi}{n}}$ où k est un entier entre 1 et $n - 1$ premier avec n .

Le degré de ω_n est donc égal à $\varphi(n)$, nombre d'entiers entre 1 et $n - 1$ premiers avec n .

Un cas es
qui correspo

est irréducti

D'où l'équ

le poly

Les premi
à $2 + 1$, 2^2
sont pas pre
 $2^m + 1$ est
premier qui
dent à $q =$

On verra

le 2, il possède un
(38) donc une telle
ante d'extensions

ompas à partir d'un
s de son polynôme
ifie que le corps de
une puissance de 2.

m, qui est le degré
ici la condition est

sur $\mathbb{Q}$, il s'exprime
général à l'aide de
rniens intervient, z

pe de Galois du
divisible par 3 (voir
soit résoluble par
le des racines n'est
ompas.

$$\frac{-1}{-1}$$

ue d'ordre 4. Donc

e à la règle et au
entagone régulier

régulier de n côtés

pend du groupe de

base $\mathbb{Q}$ si l'on part

ndice n , ses racines

k est un entier entre

l et $n - 1$ premiers

Un cas est particulièrement simple : si n est premier, $\phi(n)$ est égal à $n - 1$, ce qui correspond bien au fait que

$$\frac{X^n - 1}{X - 1} = 1 + X + \dots + X^{n-1}$$

est irréductible sur $\mathbb{Q}$, donc égal à Φ_n .

D'où l'équivalence, pour un nombre premier p

le polygone à p côtés est constructible $\Leftrightarrow p - 1$ est puissance de 2.

Les premières valeurs sont $p = 3, 5, 17, 257, 65537, \dots$, égales respectivement à $2 + 1, 2^2 + 1, 2^4 + 1, 2^8 + 1, 2^{16} + 1$. Par contre, $2^3 + 1, 2^5 + 1, \dots$, ne sont pas premiers ; d'ailleurs, si m a un diviseur impair, soit $m = (2t + 1)q$, alors $2^m + 1$ est divisible par $2^q + 1$, donc non premier, par suite tout nombre premier qui convient est de la forme $2^{2^k} + 1$ et les valeurs ci-dessus correspondent à $q = 1, 2, 3, 4$; par contre, $q = 5$ ne marche pas.

On verra en exercice le critère pour m non premier.

- La constructibilité du pentagone se vérifie dans le calcul de $e^{\frac{2i\pi}{5}}$ (voir p. 229) où n'entrent que des racines carrées.

- Par contre, dans le calcul de $e^{\frac{2i\pi}{7}}$ interviennent des racines cubiques, ce qui correspond bien à la non-constructibilité de l'heptagone : le degré de Φ_7 est 6.

Cet heptagone est le premier polygone régulier non constructible.

- L'hexagone et l'octogone le sont, car $e^{\frac{2i\pi}{6}}$ et $e^{\frac{2i\pi}{8}}$ sont égaux respectivement à

$$-j^2 = \frac{1 + i\sqrt{3}}{2} \quad \text{et} \quad \frac{1 + i}{\sqrt{2}}.$$

Seules interviennent des racines carrées (d'ailleurs, on trouve

$\Phi_6 = 1 - X + X^2$ et $\Phi_8 = 1 + X^4$).

- Les entiers entre 1 et 8 premiers avec 9 sont 1, 2, 4, 5, 7, 8, il y en a 6 : ce n'est pas là une puissance de 2, Φ_9 est de degré 6 et le polygone de neuf côtés n'est pas constructible.

- Par contre, Φ_{10} est de degré 4, et le décagone régulier est constructible.

- On remarquera que, comme on peut diviser en deux un angle à la règle et au compas, la constructibilité du polygone de n côtés implique celle du polygone de $2^m n$ côtés quel que soit l'entier m (ainsi le décagone résulte du pentagone).

- La construction du polygone de dix-sept côtés a en fait été réalisée avant même la naissance de Galois, par Gauss dont c'était là un des titres de fierté (voir p. 232).

Montrer que les seuls automorphismes laissant invariant

$$2 \cos \frac{2\pi}{n} = \omega_n + \omega_n^{-1}$$

sont l'identité et $\omega_n \rightarrow \omega_n^{-1}$.

En déduire que le degré de $\cos \frac{2\pi}{n}$, ou degré du corps fixe par ces deux automorphismes, est $\frac{\varphi(n)}{2}$.

4. Un nombre est constructible si, et seulement si, il appartient à une extension normale de degré puissance de 2 (et pas à une extension quelconque de degré puissance de 2). La constructibilité de α sur $\mathbb{Q}$ signifie que le degré de la clôture normale de $\mathbb{Q}(\alpha)$ est puissance de 2.

5. Le polygone régulier de quinze côtés est constructible.

Montrer que Φ_{15} est le quotient de $X^{10} + X^5 + 1$ par $X^2 + X + 1$, et que $2 \cos \frac{2\pi}{15}$ est racine de

$$X^4 - X^3 - 4X^2 + 4X + 1.$$

6. Étudier la trisection d'un angle de 72° .

Index alphabétique

- Caractéristique d'un corps, 69.
Clôture algébrique, 27.
 — normale, 188.
Composantes cycliques, 131.
Conjugaison
 — de corps, 162.
 — de groupes, 130.
Conjugués, 49, 96, 162, 184.
Corps
 — algébriquement clos, 27.
 — cyclotomique, 28, 122.
 — de Galois, 76.
 — de rupture, 27.
 — fixe, 212.
 — intermédiaire, 76.
Correspondance de Galois, 215.
Cycle, 130.
- Degré d'un élément, 90.
 — d'une extension, 71.
Dépendance algébrique, 25.
 — rationnelle, 25.
Déterminant de Sylvester, 42.
Discriminant, 41, 55, 205.
- Élément algébrique, 80.
 — primitif, 101.
 — transcendant, 79.
Éléments algébriquement indépendants, 25.
Équation abélienne, 253.
 — bicarrée, 178.
 — binôme, 21.
 — générale, 26.
 — résoluble, 22.
 — transformée, 44.
Extension, 10, 71.
 — algébrique, 86.
 — cyclique, 247.
 — normale, 187.
 — par radical, 24.
 — par radicaux successifs, 24.
 — quadratique, 119.
 — simple, 101.
 — transcendante, 86.
- Fonctions symétriques élémentaires, 34.
Formules de Cardan, 59.
 — de Ferrari, 66.
 — de Newton, 43.
Fraction rationnelle symétrique, 35.
- Groupe alterné, 131.
 — cyclique, 129.
 — de Galois, 137, 184.
 — dérivé, 238.
 — quotient, 130.
 — résoluble, 238.
 — symétrique, 131.
 — transitif, 142.
- Indice d'un sous-groupe, 130.
Irrationnelle accessoire, 201.
 — naturelle, 202.
- K-automorphisme, 137.
- Longueur d'un cycle, 131.
- Nombre constructible, 12.
Nombres algébriques, 24, 100.
Norme, 190.
- Ordre de multiplicité, 28.
 — d'un élément, 129.
 — d'un groupe, 129.
- Permutation cyclique, 130.
 — impaire, 131.
 — paire, 131.
- Polynôme
 — cyclotomique, 123.
 — minimum, 90.
 — normal, 183.
 — réciproque, 46.
 — séparable, 31.
 — symétrique élémentaire, 34.
 — totalement factorisable, 29.

Racine primitive de l'unité, 122.
 Radical, 21.
 — irréductible, 251.
 Réduction, 201.
 Relation rationnelle, 136.
 Résolvante de Galois, 183.
 — de Lagrange, 52.
 — partielle, 23, 181.
 Résultant, 40.

Saturation par radicaux, 22.
 Saturé, 17.
 Sous-groupe normal, 130.
 Substitution, 44.

Trace, 189.
 Translation, 44.
 Transposition, 131.

σ_i , 34.
 S_n , 37.
 $R(P, Q)$, 40.
 $P \circ f$, 44.
 $\text{car } K$, 69.
 $L : K$, 71.
 $K(\alpha)$, 72.
 $K(\alpha_1, \dots, \alpha_n)$, 7.
 $K(Q)$, 72.
 $CG(p^n)$, 76.
 $K[\alpha]$, 79.
 M_n , 82.
 $\varphi(n)$, 122.
 Φ_n , 123.
 C_m , 130.

radicaux, 22.

mal, 130.

31.

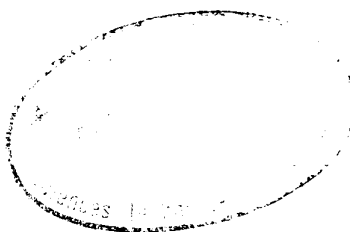
Index des notations

σ_i , 34.
 S_i , 37.
 $R(P, Q)$, 40.
 $P \circ f$, 44.
car K , 69.
 $L : K$, 71.
 $K(\alpha)$, 72.
 $K(\alpha_1, \dots, \alpha_n)$, 72.
 $K(Q)$, 72.
 $CG(p^n)$, 76.
 $K[\alpha]$, 79.
 M_n , 82.
 $\varphi(n)$, 122.
 Φ_n , 123.
 C_m , 130.

$H \triangleleft G$, 130.
 Σ_n , 131.
 A_n , 131.
 $G(P|K)$, 137.
 $G(P)$, 137.
 $K \triangleleft L$, 187.
 $T_{L|K}(x)$, 189.
 $T_L(x)$, 189.
 $T(x)$, 189.
 $N_{L|K}(x)$, 190.
 $N_L(x)$, 190.
 $N(x)$, 190.
 M_G , 212.
 $D(G)$, 238.

PHOTOCOMPOSITION : IMPRIMERIE DURAND
28600 LUISANT (FRANCE)

*Achevé d'imprimer en septembre 1980
sur presse CAMERON
dans les ateliers de la S.E.P.C.
à Saint-Amand-Montrond (Cher)*



Dépôt légal : 4^e trimestre 1980.
N° d'Édition : 4295. N° d'Impression : 972.
Imprimé en France

Cette série de monographies présente des thèmes tous plus ou moins liés à l'algèbre linéaire. Il serait certes utopique de les considérer comme indépendants les uns des autres. Toutefois, en rappelant au besoin les résultats de base nécessaires à la compréhension de chacun, il s'avère possible de traiter les différents sujets comme des entités.

A partir du niveau du baccalauréat, la série couvre tous les sujets d'algèbre linéaire imaginables durant les deux premiers cycles universitaires et les classes préparatoires aux grandes écoles. Elle aborde aussi plusieurs thèmes considérés comme du niveau supérieur à la maîtrise, mais indispensables à quiconque veut aller plus loin dans des domaines proches de l'algèbre : ainsi les extensions de corps, les produits tensoriels, les classifications de transformations, etc.

Le style d'écriture a cherché à être le plus continu possible au lieu de consister en une suite de théorèmes et de corollaires. L'idée essentielle est de faire apparaître «naturellement» le pourquoi des notions introduites et le comment des résultats prouvés, le tout étant illustré de nombreux exemples traités in extenso. Mais l'ambition connaît ses limites : l'«algèbre pour tout le monde» reste à faire. Ceci est tout au plus une tentative d'«algèbre à visage humain»...

Déjà paru :

La structure vectorielle.
Les applications linéaires.

A paraître :

Calcul matriciel.

Claude MUTAFIAN.

- né en 1942 de parents arméniens établis en France à la suite du génocide de 1915.
- ancien élève de l'École Normale Supérieure (1962-66).
- agrégé de l'Université (1965).
- a enseigné dans les Universités suivantes :
 - Université de Paris-Sud (1965-68) ;
 - Princeton University - USA (1968-69) ;
 - Universidad de la Habana - Cuba (1969-71) ;
 - Universidad Nacional Autónoma de México (1975-76) ;
 - Université d'état d'Erevan - Arménie soviétique (1980) ;
 - Université de Paris-Nord (depuis 1971).

ISSN : 022

ISBN : 2-7

la Villette



048194